NIST Cybersecurity White Paper
NIST CSWP 34 ipd

Mitigating Cybersecurity and Privacy Risks in Telehealth Smart Home Integration:

Healthcare and Public Health Sector Risk Management Approaches

Initial Public Draft

Ronald Pulivarti
Applied Cybersecurity Division
Information Technology Laboratory

Kevin Littlefield
Bronwyn Patrick
Sue Wang
Ryan Williams
The MITRE Corporation

This publication is available free of charge from:
https://doi.org/10.6028/NIST.CSWP.34.ipd

November 6, 2024

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Certain equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

How to Cite this NIST Technical Series Publication:
Pulivarti R, Littlefield K, Patrick B, Wang S, Williams R (2024) Mitigating Cybersecurity and Privacy Risks in Telehealth Smart Home Integration: Healthcare Sector Risk Management Approaches. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 34 ipd. https://doi.org/10.6028/NIST.CSWP.34.ipd

Author ORCID iDs
Ronald Pulivarti: 0000-0002-8330-3474
Kevin Littlefield: 0009-0007-2168-6282
Bronwyn Patrick: 0009-0001-7885-4773
Sue Wang: 0000-0003-4587-429X
Ryan Williams: 0009-0007-5158-309X

Public Comment Period
November 6, 2024 – January 6, 2025

Submit Comments
hit_nccoe@nist.gov

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

Additional Information
Additional information about this publication is available at Mitigating Cybersecurity Risk in Telehealth Smart Home Integration, including related content, potential updates, and document history.

All comments are subject to release under the Freedom of Information Act (FOIA).

Abstract

In-patient service demands have increased during a time when patients have experienced reduced access to hospital care. Hospital-at-Home (HaH) solutions provide an in-patient care experience for patients, which may result in reduced costs and improved outcomes. While these are desirable benefits, HaH involves privacy and cybersecurity risk by introducing medical device-grade equipment and information systems into environments the hospital does not control, i.e., the patient's home. Patient homes may include a growing number of Internet of Things (IoT) devices as part of their "smart home" environment. IoT devices may be used as pivot points into a hospital's information system environment. IoT devices are a novel set of computing devices that do not allow patients or HaH implementors to provision commonly accepted privacy and security practices. This paper examines privacy and cybersecurity risks found in HaH deployments when using smart speakers as a representative IoT device and provides recommended steps to address those risks. This paper describes applying controls that include access control, authentication, continuous monitoring, data security, governance, and network segmentation.

These practices include steps that the hospital can take to segment HaH equipment and data from other personally owned devices in the patient's home and implement phishing-resistant authentication. Personally owned devices may be prone to compromise and would affect healthcare systems without appropriate segmentation. Also, voice-enabled technologies may be prone to identity spoofing or permitting unauthorized individuals to access HaH equipment or health information.

Keywords

Application Programming Interface; API; biometric devices; cybersecurity; data privacy; data privacy and security risks; healthcare delivery organization; HDO; Hospital-at-Home; HaH; Internet of Things; IoT; smart home; telehealth; voice assistant.

Audience

This document provides guidance to technologists and information security professionals that work in healthcare delivery organizations (HDOs), including hospitals, clinics, or other healthcare facilities that may implement Hospital-at-Home solutions for their patients.

Note to Reviewers

This document presents the draft *NIST Cybersecurity White Paper (CSWP) for Mitigating Cybersecurity and Privacy Risks in Telehealth Smart Home Integration*. This paper is designed to provide recommendations for enhancing the protection of patient data and hospital infrastructures. It aligns with various NIST guidance and frameworks to provide actionable insights for healthcare organizations that implement smart home integration (SHI) workflows.

We are seeking feedback on the following concepts presented in this paper:

1. What information would be valuable for you in understanding and applying these security and privacy capabilities?
2. How do you expect this guide to influence your future practices and processes?
3. How do you envision using this guide? What changes would you like to see to increase/improve that use?
4. What cybersecurity or privacy capabilities would you most likely implement when integrating SHI workflows?

Table of Contents

List of Tables

List of Figures

Acknowledgments

National Institute of Standards and Technology (NIST) and the National Cybersecurity Center of Excellence (NCCoE) would like to thank Nakia Grayson, Jeff Marron, Cherilyn Pascoe, Isabella Tai, and Hannah Zook of the NIST Applied Cybersecurity Division and Jeremy Miller, Chris Peloquin, Julie Snyder, and Theresa Suloway of the MITRE Corporation for their contributions to this paper.

Executive Summary

Healthcare Delivery Organizations (HDOs) have begun implementing Hospital-at-Home (HaH) programs for select patients. HaH is a form of telehealth wherein patients receive in-patient care, including clinical care and monitoring, at their place of residence. Healthcare systems, often in collaboration with partner organizations, incorporate communication interfaces, patient monitors, and other medical devices into the patient's residence to provide advice, engage with the patient, and perform clinical care while leveraging the advantages associated with that patient receiving treatment in a location amenable to the patient.

HaH combines elements found in telehealth solutions with components such as hospital-grade medical devices typically found in in-patient settings. HaH integrates with commercial solutions procured by the patient to enhance their lives. An example of patient-procured solutions includes Internet-of-Things (IoT) devices. This paper uses a smart speaker device as a representative IoT device that may be found in the patient's home. This paper considers privacy and cybersecurity risks associated with smart speaker inclusion, both as a general IoT device that is not managed by the HDO and as a device that the patient uses to communicate with care providers and retrieve health information.

Adversaries may use patient-procured IoT devices and network infrastructures as a pivot into an HDO's environment. The objective of this paper is to examine privacy and cybersecurity risks present in IoT devices, as they exist in the same environment as in-patient-grade medical devices. Both patient-procured and medical devices may have vulnerabilities that cannot be easily addressed through regular patch cycles. This paper examines risks and mitigation approaches.

This paper uses NIST guidance in framing risks and proposing mitigating controls. The National Cybersecurity Center of Excellence (NCCoE) healthcare team applies guidance from the *National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0* (CSF 2.0) [1], the *NIST Privacy Framework* (PF) [2], and *NIST Internal Report (NISTIR) 8425 Profile of the IoT Core Baseline for Consumer IoT Products* [3] as well as concepts discussed in previous NCCoE practice guides.

A core theme found in other NCCoE healthcare-related practice guides and NIST guidance documents, for example, calls upon HDOs to ensure network segmentation between medical devices and other environments. Network segmentation impedes a threat actor's ability to compromise an endpoint and then promulgate to other devices. Another concern that this paper highlights is the need to limit access to authorized individuals. HaH deployments involve using hospital-grade medical devices in patient's home environments that have not been designed to host sensitive systems or devices such as medical devices. This paper discusses identity and access controls that assure the HDO that health data are only accessed by authorized individuals and devices.

HaH is a new mode of care delivery that may improve patient outcomes. HaH allows patients to access the same level of care found in an in-patient setting while in the comfort of their own homes. By implementing the safeguards suggested in this paper, HDOs will reduce their risk profile while providing a valued service to their patients.

1. Introduction

Healthcare Delivery Organizations (HDOs) have begun implementing Hospital-at-Home (HaH) programs for select patients [4][5]. HaH is a form of telehealth wherein patients receive in-patient care, including clinical care and monitoring, at their place of residence. Healthcare systems, often in collaboration with partner organizations, incorporate communication interfaces, patient monitors, and other medical devices into the patient's residence to provide advice, engage with the patient, and perform clinical care while leveraging the advantages associated with that patient receiving treatment in an amenable location.

Telehealth encompasses many potential use cases. Home healthcare, similar to HaH, is another example. Home healthcare uses consumer-grade technology and empowers patients to take an active role in managing their health. Technologies may include on-demand access to clinicians via web conferencing or using consumer-grade heart monitoring, blood pressure gauges, or blood oxygen sensors. Consumer-grade devices may be embedded in small-footprint devices, smart devices, health activity wearables, or similar technologies [6].

HaH differs from home healthcare in that it focuses on hospital-grade medical devices. While consumer-grade devices may be used as part of an overall solution (e.g., using smartphones, tablets, laptops, or other computing endpoints), HaH is a prescriptive solution where an HDO deploys medical devices to the patient's home and may use communication infrastructure and consumer-grade interfaces to better provide an in-patient care experience. Using consumer-grade devices, such as smart speakers, in the patient's home in combination with the HaH hospital-grade medical devices is what this paper considers telehealth smart home integration.

HaH offers HDOs several benefits that include improving patient outcomes, alleviating in-patient bed capacity limits, and providing safety for patients and care team members during infectious scenarios. Nevertheless, HaH presents several cybersecurity and privacy challenges that this paper discusses along with proposed mitigation approaches. While this paper explores cybersecurity and privacy risks and mitigation approaches, HDOs should be aware that other technology challenges will need to be addressed, which are not covered in this paper. Examples of these challenges concern the communications spectrum or ensuring appropriate communications quality of service. While HaH provides pathways that allow HDOs to improve the patient care experience, HDOs should consider a comprehensive set of risks when developing an HaH program.

This paper examines an HaH use case where patients use voice assistants (smart speakers) to interact with a care team. This telehealth smart home integration use case analyzes scenarios where a patient procures a smart speaker. The patient's home environment will include hospital-grade medical devices, including remote patient monitoring. The hospital deploys an HaH solution using a third-party solution provider [1] that leverages a natural language processing (NLP) interface with the smart speaker. By focusing on the cybersecurity and privacy risks that may be found in this use case, the National Cybersecurity Center of Excellence (NCCoE) healthcare team applies guidance from the *National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0* (CSF 2.0) [1], the *NIST Privacy Framework* (PF)

[2], and *NIST Internal Report (NISTIR) 8425 Profile of the IoT Core Baseline for Consumer IoT Products* [3].

2. Telehealth Smart Home Integration Ecosystem

This paper considers telehealth solutions that use voice assistants or smart speakers in the patient's home as interfaces into health information systems. The paper assumes that the patient is receiving treatment at their home and, therefore, is regarded as an in-patient by the hospital. The health information systems are provisioned in a multi-domain environment (as shown in Figure 1) that consists of four separate domains:

- Patient Home
- Voice Assistant Platform
- Healthcare Integration Solution
- HDO

The patient's home contains a patient-provided voice assistant that the patient will use to interact with the HDO. The patient's home also contains HDO-provisioned medical and biometric devices to monitor the patient's vitals and the patient's personal devices, such as mobile phones, game consoles, and Internet of Things (IoT) devices. The patient can use the voice assistant to interact with the HDO and perform actions such as completing a daily check-in, scheduling an appointment with their provider, or refilling a prescription. Once the patient activates the voice assistant to perform an action, a recording of their voice is sent to the voice assistant platform for processing.

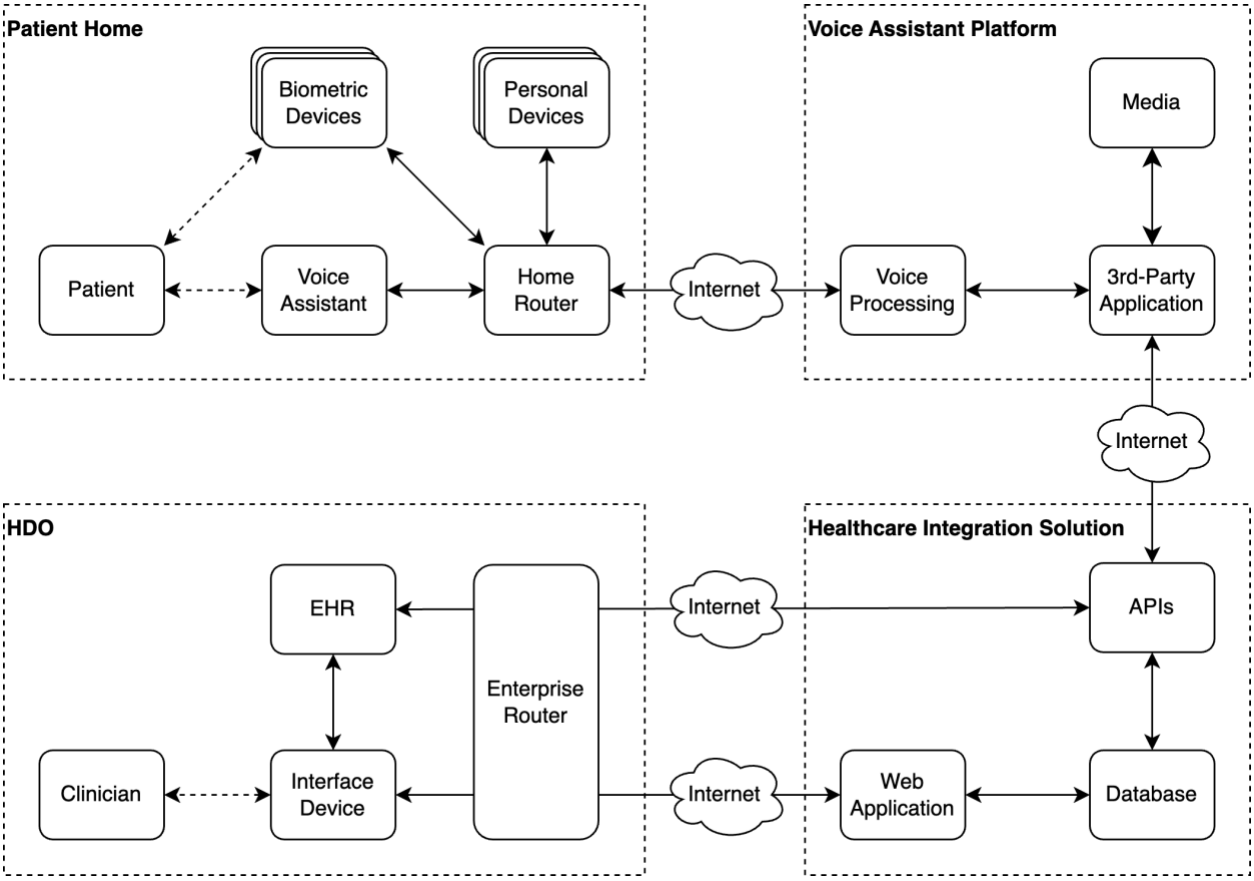
The voice assistant platform contains all the backend services that the voice assistant uses to interpret patient commands and perform actions. This includes voice processing services such as NLP (speech-to-text, text-to-speech, etc.) as well as the infrastructure to route the patient's request to the correct third-party application. The voice assistant platform also hosts the third-party application, along with any media the application uses (video, audio, etc.), which interacts with the healthcare integration solution and HDO to facilitate the patient's actions.

The healthcare integration solution is managed by a third-party provider and contains the necessary components to connect the patient to the HDO through the voice assistant platform. These components include application programming interfaces (APIs) that the third-party application uses to interact with servers hosted by the healthcare integration solution as well as the HDO-hosted electronic health record (EHR) server. Through the APIs, the third-party application can pull information about the patient, such as their prescribed medications, daily check-in questions, and provider's schedule. Based on the patient's request, the third-party application can also update the EHR and other data repositories by submitting the patient's daily check-in answers or scheduling an appointment.

The HDO contains the patient's healthcare provider as well as the EHR server that manages the patient's health data. The EHR server contains its own APIs that allow external applications to interact with it to perform specific actions, such as retrieving or modifying patient data. In some

situations, the EHR can also connect to the healthcare integration platform through APIs to collect and store patient information. From the HDO, the healthcare provider can access the EHR or the healthcare integration solution through an interface device such as a phone, tablet, or computer.

Figure 1 - High-Level Smart Home Integration Reference Architecture



3. Smart Home Integration Ecosystem Risk Analysis

HDOs need to examine several risks associated with implementing an HaH solution. HDOs need to consider all potential risks, including the financial and operational risks that are beyond the scope of this paper. Risks need to be weighed against benefits that may lead to improved patient outcomes. This paper limits its risk analysis to cybersecurity and privacy concerns.

This paper frames its risk analysis by applying concepts found in NIST Special Publication 800-30 Revision 1, *Guide for Conducting Risk Assessments* [7]. The guide provides definitions for core concepts that hospitals should consider when performing risk analysis. NIST 800-30 discusses using “risk models” that examine threats, vulnerabilities, likelihood, and impact. NIST 800-30 provides a generic risk model that shows a threat source representing an adversarial actor as an initial trigger. The threat source initiates a threat event that exploits one or more vulnerabilities found in an asset. Successful vulnerability exploitation in this chain causes adverse impacts that result in organizational risk.

Controls may be implemented that limit a threat event's likelihood, address or limit asset vulnerabilities, or manage adverse impact. This paper uses the high-level reference architecture that decomposes the HaH system into components found in four distinct domains, as described in Section 2. Next, this paper considers threats and respective risks and recommends contextualized risk mitigation controls.

Vulnerabilities are specific to components, e.g., by the manufacturer and versions. In this paper, the NCCoE assumes that components may include vulnerabilities. A common control recommendation would entail that HDOs perform appropriate vulnerability or patch management, which may pose challenges considering that some HaH components are medical devices where patches are not readily available. This paper's controls focus, therefore, highlights controls that reduce threat event likelihood or adverse impact mitigation.

3.1. Sample Threat Events

As HDOs implement technologies such as HaH or other innovative solutions, they should apply risk assessment guidance as described in NCCoE practice guides. The NCCoE applied a risk assessment and performed an analysis of the smart home integration ecosystem, identifying several cybersecurity and privacy challenges along with proposed mitigation approaches. The following list shows threat events that may cause those cybersecurity and privacy challenges within the SHI integration ecosystem.

- **Data Exfiltration:** An unauthorized actor impacts patient data confidentiality and disassociability by intercepting unencrypted communications from a voice assistant to obtain personal identifiable information (PII) or protected health information.
- **Data Manipulation:** An unauthorized actor compromises patient data integrity and manageability by intercepting and manipulating data communications between the voice assistant, health integration solution, and hospital information systems or by exploiting insecure API configurations.
- **Denial of Service:** An unauthorized actor disrupts the voice assistant communication ecosystem's availability and predictability by flooding the health integration solution platform or hospital information systems with API requests, causing the system to not function as expected.
- **Operating system (OS) or application disruption:** An unauthorized actor decreases patient data integrity, system availability, and data or system predictability by altering commands sent to the health integration solution, leading to incorrect processing of patient requests and erroneous actions in hospital information systems.
- **Unauthorized Access:** An unauthorized individual compromises patient data confidentiality and manageability by accessing a patient's voice assistant device through their home network or weak physical authorization controls.

Figure 2 depicts a high-level reference architecture for the smart home integration case. The architecture shows four domains: the patient home, the voice assistant platform, the healthcare integration solution, and the HDO. The architecture diagram applies an overlay that

aligns with areas where threat events may be present. The five threat types that the diagram portrays are Data Exfiltration, Data Manipulation, Denial of Service, OS/Application Disruption, and Unauthorized Access.

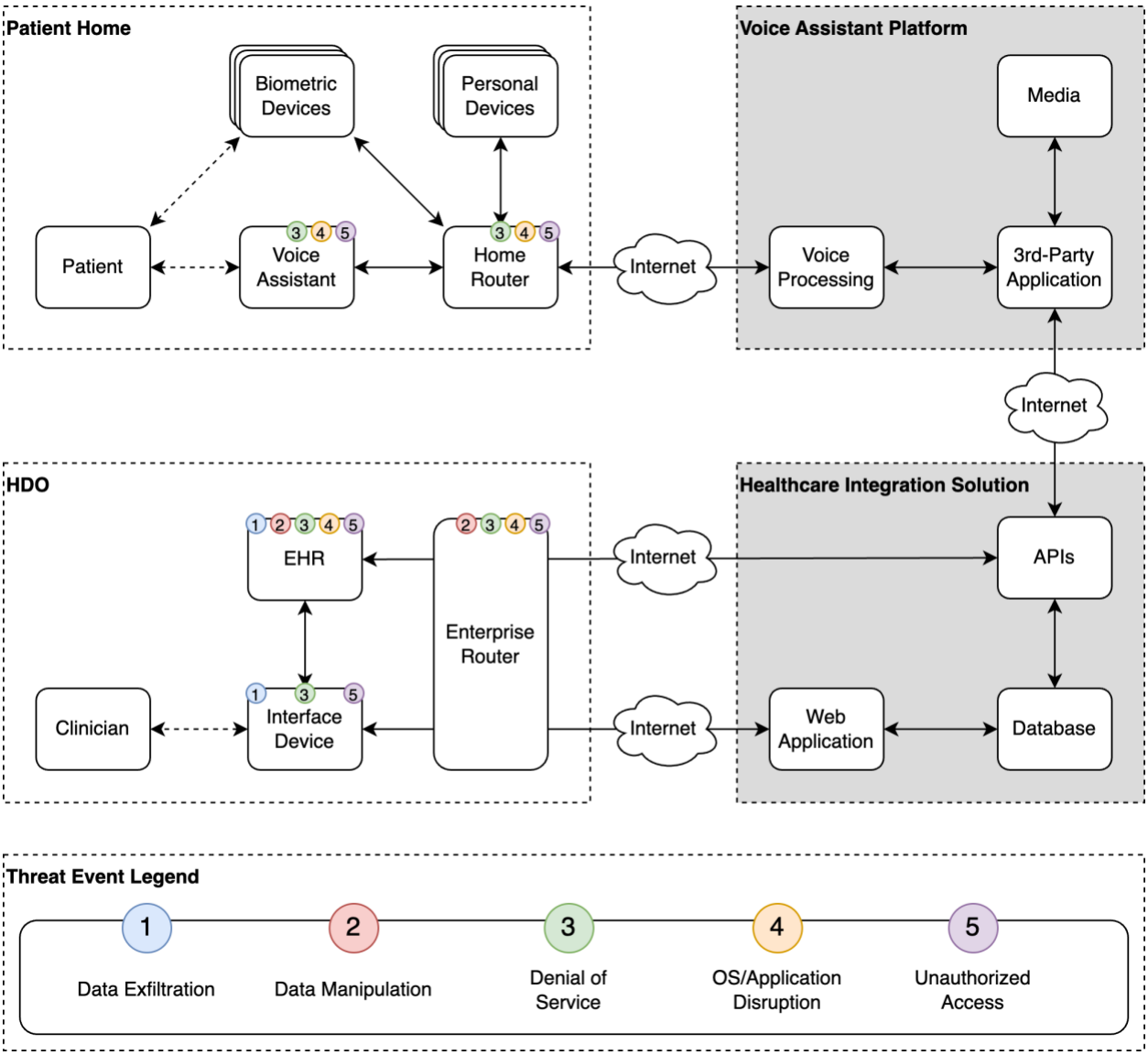
This paper examines threats that exist in the patient's home and HDO environments. While the voice assistant platform and the health integrator environment will have present threats, these threats need to be addressed by the respective suppliers. HDOs should be aware of how their suppliers and partners manage risk beyond the topics discussed in this paper.

In the patient's home domain, the voice assistant may be prone to denial of service, OS/application disruption, or unauthorized access. The diagram also depicts a home router component that would operate as the home network's backbone and means to connect to the internet. The home router may be prone to these same threats found in the voice assistant.

Figure 2 shows the HDO environment that includes EHR, an interface device used by a clinician, and an enterprise router that represents the HDO's network infrastructure and network communications component that enables Internet connectivity. The diagram depicts the EHR as subject to data exfiltration, data manipulation, denial of service, OS/application disruption, and unauthorized access. The interface device may be subject to data exfiltration, denial of service, and unauthorized access. The enterprise router is depicted as being subject to data manipulation, denial of service, OS/application disruption, and unauthorized access.

The threats discussed in this paper are representative. HDOs implementing HaH solutions may identify different threats and expand on the threat types and components that may be affected when performing respective risk assessments.

294 **Figure 2 - High-Level Reference Architecture (with Threat Events)**



295 ## 3.2. Recommended Cybersecurity and Privacy Practices

296 To address the cybersecurity and privacy challenges as a result of the threat events discussed in
297 the previous section for the smart home integration ecosystem, this paper proposed mitigation
298 approaches and identified controls aligned with the sample threat events.

299 This paper applies guidance from the CSF 2.0 [1], the PF [2], and NISTIR 8425 [3]. The
300 recommended controls include access control, authentication, continuous monitoring, data
301 security, governance, and network segmentation. To provide a comprehensive understanding,
302 Table 1 below details the recommended controls and their descriptions with a focus informed
303 by the CSF 2.0, PF, and IoT points of views.

304 **Table 1: Recommended Cybersecurity and Privacy Practices**

Recommended Control	Control Description
Access Control	[CSF Focus] By implementing the principle of least privilege for both users and systems, the likelihood of excessive agency or privilege escalation is reduced. Enabling multifactor authentication on HaH endpoints reduces the likelihood of unauthorized individuals accessing HaH technologies and health information. These forms of access control ensure that only authorized individuals can access specific resources, which protects patient data from unauthorized access or alteration and maintains data confidentiality and integrity. [PF Focus] This supports the manageability goal by allowing granular administration of PII and the predictability goal by enabling reliable assumptions about PII processing. [IoT Focus] Consumer IoT products (e.g., voice assistant) restrict logical access to local and network interfaces – and to protocols and services used by those interfaces – to only authorized individuals, services, and IoT product components. An IoT product is defined as an IoT device or IoT devices (e.g., voice assistant) and any additional product components (e.g., companion mobile app, cloud backend) that are necessary to use the IoT device beyond basic operational features.
Authentication	[CSF Focus] Implementing Zero Trust concepts in the HaH workflow forces all devices and users to authenticate themselves before interacting with hospital information systems and data. This authentication process enhances security by verifying identities before granting access, thus preventing unauthorized access and safeguarding patient data's integrity and confidentiality. [PF Focus] This supports the predictability goal by ensuring reliable assumptions about who can access PII. [IoT Focus] Consumer IoT products (e.g., voice assistant) restrict logical access to local and network interfaces – and to protocols and services used by those interfaces – to only authorized individuals, services, and IoT product components.
Continuous Monitoring	[CSF Focus] By continuously tracking and analyzing network traffic, network monitoring can identify and respond to unusual activities, such as a sudden surge in traffic that may indicate a Denial-of-Service attack. This control allows for more immediate action to be taken to mitigate the attack, thereby minimizing disruption to services and maintaining the availability of critical health information system functionality and data for patients and clinicians. [PF Focus] This supports the predictability goal by ensuring the system operates as expected. [IoT Focus] Consumer IoT products (e.g., voice assistant) support the detection of cybersecurity incidents affecting or affected by IoT product components and the data they store and transmit.
Data Security	[CSF Focus] Implementing data encryption across the smart home integration workflow for both data-in-transit and data-at-rest is a crucial data security measure. It protects sensitive patient data during storage and transmission, maintaining data

Recommended Control	Control Description
	confidentiality and integrity and preventing unauthorized actors from accessing or altering the data. [PF Focus] This supports the disassociability goal by ensuring PII is processed without association with individuals beyond operational requirements. [IoT Focus] Consumer IoT products (e.g., voice assistant) protect data stored across all IoT product components and transmitted both between IoT product components and outside the IoT product from unauthorized access, disclosure, and modification.
Governance	[CSF Focus] It is important to keep track of all hospital information system components and their setup. Implementing rules and procedures for managing and securing data is also crucial. Appropriate asset and configuration tracking helps ensure hospital information systems follow regulations, reduce risks, and improve overall system safety. Since hospital information system APIs often have more access points than traditional web applications, it's important to have up-to-date documentation and a list of all the systems and API versions being used. This helps avoid problems like outdated API versions and exposed access points. [PF Focus] This supports the predictability and manageability goal by allowing granular administration of PII in accordance with the stated purposes of collection. This also helps ensure PII collected unintentionally is handled appropriately in accordance with data minimization and retention policies. [IoT Focus] Throughout the development lifecycle, the IoT product developer creates or gathers and stores information relevant to the cybersecurity of the IoT product and its product components. Additionally, the IoT product developer broadcasts (e.g., to the public) and distributes (e.g., to the customer or others in the IoT product ecosystem) information relevant to cybersecurity.
Network Segmentation	[CSF Focus] Creating network zones in the patient's home to separate personally owned IoT devices from hospital-managed Internet of Medical Things devices is a form of network segmentation. This approach divides the home network into smaller parts, limiting unauthorized access to sensitive data and reducing the impact of a breach. Attackers can only access data in the compromised segment, not the entire network. [PF Focus] This supports the disassociability goal by limiting the association of PII to individuals or devices beyond operational requirements. [IoT Focus] Consumer IoT products (e.g., voice assistants) prevent unauthorized transmissions or access to other product components. To achieve this, the consumer IoT product may need to be uniquely identified and have the ability for authorized individuals (i.e., customers), services, and other IoT product components to change the configuration settings.

3.3. Assess Cybersecurity and Privacy Control Coverage

This paper evaluates the recommended control coverage by applying the NIST CSF 2.0 [1], the PF [2], and NISTIR 8425 [3] to the identified threat events in Section 3.2 and map the

recommended controls provided in Section 3.2 to CSF 2.0 and PF Categories and Subcategories and IoT device capabilities and sub-capabilities from NISTIR 8425.

Both the CSF 2.0 and the PF share a foundation where they identify Functions, Categories, and Subcategories. The NIST PF follows the NIST CSF's established convention of labeling functions with a two-letter unique identifier. This white paper uses the Identify and Protect Functions that are described in both frameworks. Further, this paper applies the Govern and Detect functions described in the CSF 2.0 as well as the Control and Communicate functions described exclusively in the PF.

Additionally, this paper lists capabilities from NISTIR 8425 that are applicable to the controls provided in Section 3.2. NISTIR 8425 defines the cybersecurity capabilities expected of consumer IoT products (e.g., voice assistants) and IoT product developers. An IoT product is defined as an IoT device or devices and any additional product components (e.g., cloud backend, mobile app) necessary to use the IoT device beyond basic operational features. The capabilities are recommended to apply to the IoT product overall and to each IoT product component, as appropriate.

The mapping between the recommended controls identified in Section 3.2 and NIST CSF 2.0 [1], PF [2], and NISTIR 8425 [3] can be found in the Assess Cybersecurity and Privacy Control Coverage table.

4. Security Reference Architecture

Figure 3 depicts the high-level reference architecture for a smart home integration ecosystem. The architecture is made up of four domains: the patient's home, the voice assistant platform, the healthcare integration solution, and the HDO. The diagram presents an overlay that indicates where this paper recommends implementing security and privacy controls to mitigate potential threats. These security and privacy controls include access control, authentication, continuous monitoring, data security, governance, and network segmentation.

This paper highlights controls that could be implemented in the patient's home and HDO environments. While the voice assistant platform and the health integrator environment will require security and privacy controls, these controls need to be addressed by the respective suppliers. HDOs should be aware of how their suppliers and partners implement cybersecurity and privacy mitigations beyond the topics discussed in this paper.

In the patient's home, HDOs may implement security controls that include access control, authentication, data security, and network segmentation that provide safeguards for patient interactions with the voice assistant and biometric devices. The patient's home should include network segmentation that separates the HDO-provided biometric devices from the patient's home network. This segmentation may be implemented by placing an HDO-managed router between the devices and the patient's home router. Network segmentation, a concept discussed in NIST SP 1800-30, *Securing Telehealth Remote Patient Monitoring Ecosystem* [8], isolates the biometric devices from potential threats on the patient's home network and ensures that HaH components communicate with authorized services and endpoints only. Network segmentation, a concept discussed in NIST SP 1800-30 [8], isolates the biometric

devices from potential threats on the patient's home network and ensures that HaH components only communicate with authorized services and endpoints.

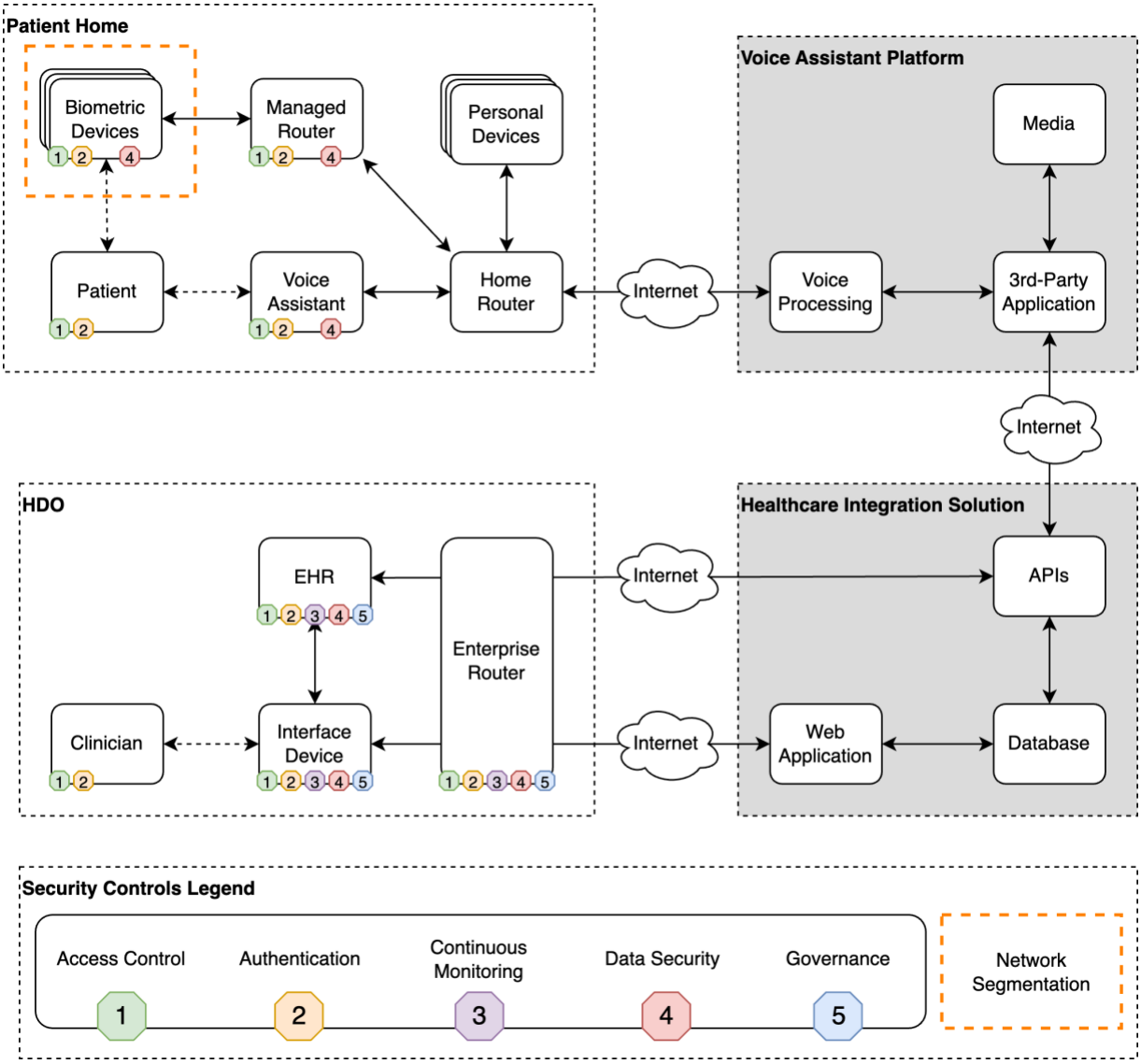
Access control and authentication are also important in the patient's home domain. HDO-provided biometric devices should restrict access to only authorized individuals. Biometric devices are intended to obtain health data from a specified patient and therefore should implement methods to ensure that data captured by these devices pertain to the patient only. Network communications to the HDO should be limited. The solution should implement configurations ensuring that only authorized devices can relay data to the HDO. Communications may be relayed through an HDO-managed router.

Security concepts should also apply to the voice-enabled application the patient interacts with, through their voice assistant, to communicate with the HDO. While it is not reasonable to physically segment the patient-owned voice assistant from the home network, HDOs should ensure that only the patient can access their own medical data through the voice-enabled application. Finally, this paper recommends implementing data security controls in the form of data encryption for any communication between the patient's home and other domains.

If HDOs will be deploying routers to patient homes, it is recommended that HDOs acquire and deploy routers that conform with the requirements in NIST IR 8425A, Recommended Cybersecurity Requirements for Consumer-Grade Router Products [9]*. Routers serve as the gatekeepers of our networks, managing the flow of data between devices in the home or office and the internet. A compromised router opens the door to a host of potentially exploitable vulnerabilities and impacts, making router cybersecurity of paramount importance in today's interconnected world.*

In the HDO, this paper recommends comprehensive security and privacy controls. A comprehensive control set includes access control, authentication, continuous monitoring, data security, and governance. All five controls have been applied to the EHR, interface device, and enterprise router/network. Any endpoint connected to the HDO network should be authenticated, monitored, and managed using mature inventory and asset management practices. Sensitive data stored or shared internally or externally should be secured through encryption. This paper also recommends that the HDO workforce members associated with providing HaH care be properly authenticated to the devices and systems they use and only have access to the resources needed for their work.

372 **Figure 3 - High-Level Reference Architecture (with Recommended Controls)**



373 ## 5. Conclusion

374 HaH presents cybersecurity and privacy risks that hospitals must consider [8]. As shown in this
375 paper, HaH and smart home integration involve interconnecting disparate environments not
376 managed directly by the hospital. HDOs depend upon third parties to provide application
377 functionality and integration into a hospital's health information system. For example, Smart
378 speaker manufacturers may control the endpoint configuration, enabling user interface
379 capabilities by providing the mechanism for NLP and interpreting commands that integrate with
380 application functionality. They may also provide audio interpretation to the patient, enabling an
381 ambient computing experience. Each of these environments offers landscapes that are prone to
382 cyber-attack and disruption.

This paper examined an HaH use case involving smart home integration as a holistic system and analyzed a sample HaH environment for potential cyber and privacy risks. The NCCoE identified potential risk mitigation controls. As part of this paper's risk analysis, the NCCoE examined some threats that HaH deployments need to consider:

- Data exfiltration
- Data manipulation
- Denial of service
- Operating system or application disruption
- Unauthorized access

This paper uses guidance found in the NIST CSF 2.0 [1], NIST PF 1.0 [2], and NISTIR 8425 [3] to identify controls that HDOs could employ to mitigate risks resulting from an adversary successfully leveraging one or more of the identified threats. This paper highlights the following recommended security and privacy controls:

- Access control
- Authentication
- Continuous monitoring
- Data security
- Governance
- Network segmentation

As noted in this paper, HaH deployments include other risks for hospitals to consider beyond cybersecurity and privacy. Hospitals should be aware that they must address operational and patient safety concerns with appropriate practices such as safeguarding health information systems, educating patients on how their data is used, and providing patients the opportunity to opt in or out of a telehealth HaH program. Patients enrolled in a HaH program should be aware of recommended cybersecurity practices that can be applied to their home networks and devices and guard themselves against traditional spoofing tactics malicious actors adopt.

HaH offers both opportunities and challenges. While it allows for personalized and convenient patient care, the threat landscape includes unconsidered cybersecurity and privacy threats. This paper has identified representative threats and proposed mitigation strategies based on NIST Frameworks and IoT publications. Hospitals considering HaH should ensure applying respective risk assessment and control selection. This paper provides guidance using NIST frameworks. Hospitals, however, need to ensure that they contextualize their risk management approach based on the challenges they face.

References

[1] National Institute of Standards and Technology (2024) *The NIST Cybersecurity Framework (CSF) 2.0.* Available at https://doi.org/10.6028/NIST.CSWP.29

[2] National Institute of Standards and Technology (2021) *NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0.* Available at https://doi.org/10.6028/NIST.CSWP.01162020

[3] Michael F, Katerina M, Paul W, Jeffrey M, Barbara C (2022). *Profile of the IoT Core Baseline for Consumer IoT Products* (National Institute of Standards and Technology, Gaithersburg, MD), NIST Internal Report (NIST IR) 8425. Available at https://doi.org/10.6028/NIST.IR.8425

[4] American Hospital Association (2020) *The Value Initiative Issue Brief Creating Value by Bringing Hospital Care Home.* Available at https://www.aha.org/system/files/media/file/2020/12/issue-brief-creating-value-by-bringing-hospital-care-home_0.pdf

[5] Food and Drug Administration (2024) *FDA Launches Health Care at Home Initiative to Help Advance Health Equity.* Available at https://www.fda.gov/medical-devices/medical-devices-news-and-events/fda-launches-health-care-home-initiative-help-advance-health-equity

[6] Medicare.gov *Home health services*. Available at https://www.medicare.gov/what-medicare-covers/whats-home-health-care

[7] National Institute of Standards and Technology (2012). NIST Special Publication 800-30 Revision 1, *Guide for Conducting Risk Assessments*. Available at https://doi.org/10.6028/NIST.SP.800-30r1

[8] Cawthra J, Grayson N, Pulivarti R, Hodges B, Kuruvilla J, Littlefield K, Snyder J, Wang S, Williams R, Zheng K (2022) Securing telehealth remote patient monitoring ecosystem. (National Institute of Standards and Technology (U.S.), Gaithersburg, MD), NIST SP 1800-30, p NIST SP 1800-30. https://doi.org/10.6028/NIST.SP.1800-30

[9] Michael F, Katerina M, Paul W, Jeffrey M, Barbara C, David L, Brad H, Chris E (2024). *Recommended Cybersecurity Requirements for Consumer-Grade Router Products* (National Institute of Standards and Technology, Gaithersburg, MD), Draft NIST Internal Report (NIST IR) 8425A ipd. Available at https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8425A.ipd.pdf

Appendix A. List of Symbols, Abbreviations, and Acronyms

API
Application Programming Interface

CSF 2.0
NIST Cybersecurity Framework 2.0

CSWP
Cybersecurity White Paper

EHR
Electronic Health Record

HaH
Hospital-at-Home

HDO
Healthcare Delivery Organization

IoT
Internet of Things

NCCoE
National Cybersecurity Center of Excellence

NIST
National Institute of Standards and Technology

NISTIR
NIST Internal Report

NLP
Natural Language Processing

OS
Operating System

PF
NIST Privacy Framework

PII
Personal Identifiable Information

SHI
Smart Home Integration

SP
Special Publication

TCP
Transmission Control Protocol