NIST Cybersecurity White Paper
NIST CSWP 34

Mitigating Cybersecurity and Privacy Risks in Telehealth Smart Home Integration

Final

Ronald Pulivarti
Applied Cybersecurity Division
Information Technology Laboratory

Kevin Littlefield
Bronwyn Patrick
Sue Wang
Ryan Williams*
The MITRE Corporation

*Former employee: all work for this publication was done while at employer.

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

December 17, 2025

NATIONAL INSTITUTE OF
STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

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.

Publication History
Approved by the NIST Editorial Review Board on 2025-11-28

How to Cite this NIST Technical Series Publication:
Pulivarti R, Littlefield K, Patrick B, Wang S, Williams R (2025) Mitigating Cybersecurity and Privacy Risks in Telehealth Smart Home Integration (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 34. https://doi.org/10.6028/NIST.CSWP.34

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

Contact Information
hit_nccoe@nist.gov

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 are a form of telehealth that provide an in-patient care experience in patients' homes, offering the potential for improved outcomes. While these are desirable benefits, HaH involves privacy and cybersecurity risks by introducing hospital-grade medical or biometric devices and information systems outside the hospital's direct control (i.e., the patient's home). Patient homes increasingly feature Internet of Things (IoT) devices, such as voice assistants (e.g., smart speakers), as part of a broader "smart home" ecosystem. These devices may not have capabilities that support privacy and security practices and may be used as pivot points for attackers to gain access to a hospital's information system.

This paper introduces a notional high-level smart home integration reference architecture to better understand these risks. Building on NIST's prior work in telehealth security, it examines privacy and cybersecurity risks associated with HaH deployments in the context of an integrated smart home environment, focusing on voice assistants (e.g., smart speakers) as a representative IoT device and outlines several sample threat events.

To address these risks, this paper leverages the NIST Cybersecurity and Privacy Frameworks and NIST IoT Core Baseline to outline mitigation efforts for healthcare delivery organizations. The recommended mitigations include access control, authentication, continuous monitoring, data security, governance, and network segmentation.

These recommended mitigation efforts adopt NIST frameworks and guidelines. For example, it highlights actions healthcare delivery organizations (HDOs) can take to isolate HaH equipment from other personally owned devices within the patient's home to safeguard sensitive data. Without such protections, compromised, personally owned devices and voice assistants (e.g., smart speakers) may lead to unauthorized access to healthcare systems and patient information.

Keywords

Application Programming Interface; cybersecurity; data privacy; healthcare delivery organization; Hospital-at-Home; Internet of Things; IoT; smart speaker; voice assistant.

Audience

This document provides guidelines for technologists and information security professionals who work in healthcare delivery organizations (HDOs), including hospitals, clinics, or other healthcare facilities that may implement HaH solutions for their patients.

Table of Contents

List of Tables

List of Figures

Acknowledgments

National Institute of Standards and Technology (NIST) 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 Michael Ekstrom, 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, offering the potential for improved outcomes. HaH represents a form of telehealth in which patients receive in-patient level care, including clinical care and monitoring, within their own residences. To enable this, healthcare systems, often in partnership with external organizations, incorporate communication interfaces, patient monitors, and other medical or biometric devices into the patient's home. These technologies facilitate clinical care, ongoing engagement, and medical advice while allowing patients to benefit from receiving treatment in a location amenable to the patient.

HaH combines essential elements of telehealth with hospital-grade medical or biometric devices typically found in in-patient settings. These programs often integrate with commercially available solutions that patients may already use to enhance their lives, for example, Internet-of-Things (IoT) devices such as voice assistants (e.g., smart speakers), which are increasingly common in-home environments. This paper focuses primarily on the privacy and cybersecurity risks associated with incorporating such devices, both as unmanaged IoT endpoints and as tools for patient-provider communication and health information retrieval.

Adversaries may exploit patient-owned IoT devices and home network infrastructures as entry points into an HDO's broader environment. The purpose of this paper is to examine privacy and cybersecurity risks present in IoT devices that exist in the same environment as hospital-grade medical or biometric devices. Both patient-procured IoT devices and hospital-grade medical or biometric devices may have vulnerabilities that cannot be easily addressed. This paper will examine these risks and provide mitigation approaches for HDOs to consider when implementing their HaH programs.

To contextualize these risks, this publication introduces a notional high-level smart home integration reference architecture. Building on NIST's previous work in telehealth security, it examines privacy and cybersecurity concerns associated with HaH deployments in an integrated smart home environment with a focus on voice assistants (e.g., smart speakers) as a representative IoT device.

This white paper uses NIST guidelines to frame risks and propose recommended cybersecurity and privacy mitigations. The National Cybersecurity Center of Excellence (NCCoE) healthcare team applies guidelines from the *National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0* (CSF 2.0) [1], the *NIST Privacy Framework Version 1.0* (PF 1.0) [2], and *NIST Internal Report (NIST IR) 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 guideline documents, for example, calls upon HDOs to ensure network segmentation between medical or biometric devices and other environments. Network segmentation impedes a threat actor's ability to compromise an endpoint and impact other devices. This paper also highlights the need for access control to limit access to authorized individuals and devices protecting patient data from unauthorized access or alteration. To protect patient data, the organization should implement data security encryption for both data-in-transit and data-at-rest maintaining data confidentiality and integrity. Additionally, this paper highlights the importance of continuous monitoring for identifying unusual traffic patterns for a quicker response in the event of a cyber-attack. Furthermore, HDOs should have an overall cybersecurity risk management strategy implementing rules and procedures for managing and securing data. By implementing the mitigations suggested in this white paper, HDOs can reduce their risk while providing valued services 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 or biometric 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 [4]. 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 includes hospital-grade medical or biometric 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 or biometric 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, including Internet-of-Things (IoT) devices such as voice assistants (e.g., smart speakers) in the patient's home in combination with the HaH hospital-grade medical or biometric devices is what this paper considers to be 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 publication explores cybersecurity and privacy risks and mitigation approaches, HDOs should be aware that other technological challenges, such as the communications spectrum or ensuring appropriate communications quality of service will need to be addressed. 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 (e.g., 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 or biometric devices, including remote patient monitoring. The hospital deploys an HaH solution using a third-party solution provider 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 guidelines from the *National Institute of Standards* *and Technology (NIST) Cybersecurity Framework 2.0* (CSF 2.0) [1], the *NIST Privacy Framework* Version 1.0 (PF 1.0) [2], and *NIST Internal Report (NIST IR) 8425 Profile of the IoT Core Baseline for Consumer IoT Products* [3].

While technical solutions are important, it is critical for the hospital to have solid policies, processes, and practices in place that support the trust relationships with their patients to ensure they are appropriately maintained over time.

2. Telehealth Smart Home Integration Ecosystem

This paper considers telehealth solutions that use voice assistants (e.g., smart speakers) in the patient's home as interfaces into hospital health information systems. While the primary focus of the telehealth solution is used in the patient’s home, these technologies can be deployed across various care settings. The guidelines provided in this paper apply broadly to all applicable care settings and assumes that the patient is receiving treatment at their home and, therefore, is regarded as an in-patient by the hospital. The hospital health information systems are provisioned in a multi-domain environment (as shown in Fig. 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 (e.g., smart speaker) that the patient will use to interact with the HDO. The patient can use the voice assistant (e.g., smart speaker) 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. These interactions are the primary focus of this paper’s risk analysis and recommended mitigation approaches. The patient’s home environment will also contain other devices that are not part of this primary focus. These additional devices include HDO-provisioned medical or biometric devices to monitor the patient’s vitals and the patient’s personal devices, such as mobile phones, game consoles, and other Internet of Things (IoT) devices.

The voice assistant platform contains all the backend services that the voice assistant uses to interpret patient commands and perform actions, which 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 includes the necessary components to enable patient connectivity with the HDO via the voice assistant platform. These components feature application programming interfaces (APIs) through which the third-party application can interact with both servers hosted by the healthcare integration solution and the HDO-hosted electronic health record (EHR) server. Using these APIs, the third-party application can retrieve patient information, such as prescribed medications, daily check-in questions, and the provider's schedule. Additionally, based on the patient's request, the third-party application can update the EHR and other data repositories by submitting the patient's daily check-in responses or scheduling an appointment.

The HDO contains the interface device that the clinician will use to interact with 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 in order to perform specific actions, such as retrieving or modifying patient data. In some situations, the EHR can also connect to the healthcare integration solution 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.

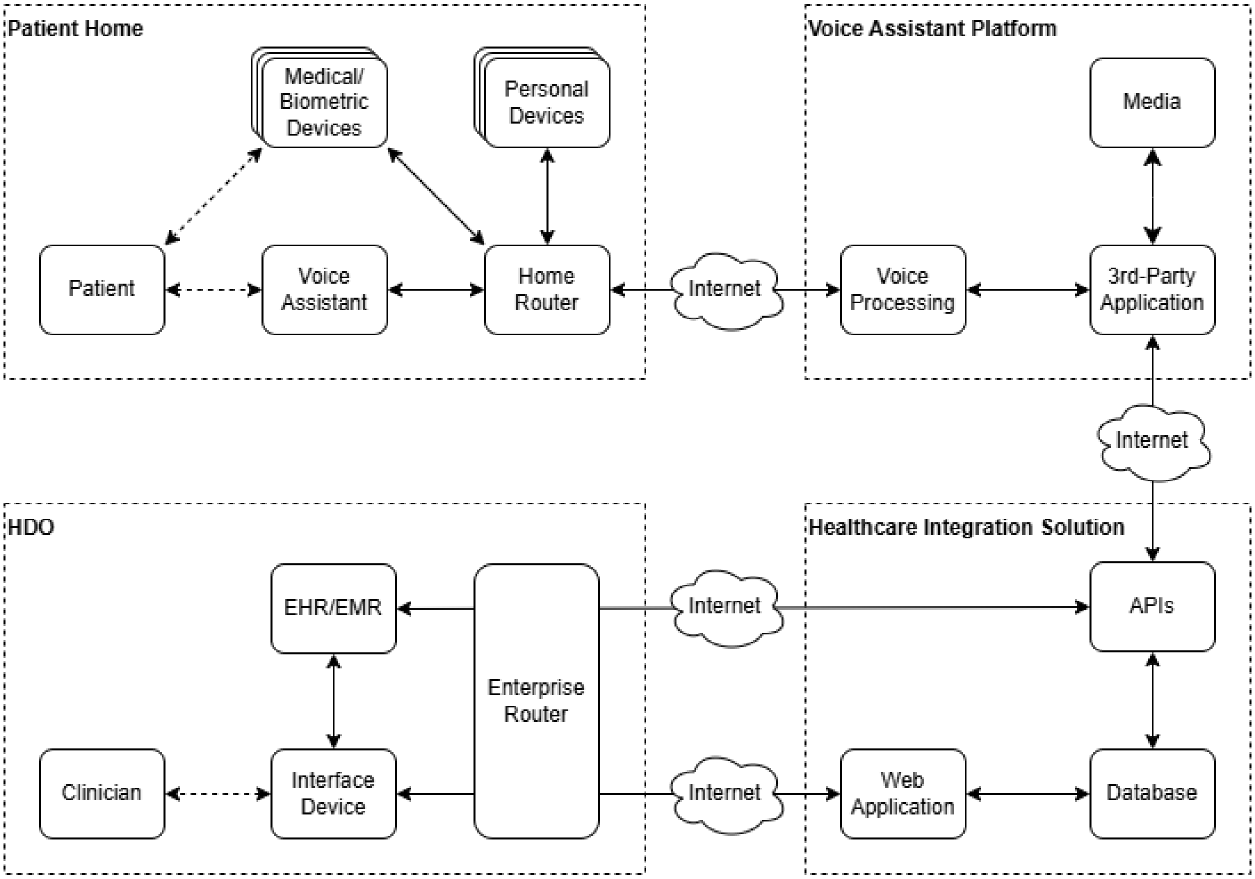

Fig. 1 - High-Level Smart Home Integration Reference Architecture

3. Smart Home Integration Ecosystem Risk Analysis

HDOs need to examine several risks associated with implementing a HaH solution. HDOs need to consider all potential risks, including 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]. It provides definitions for core concepts that hospitals should consider when performing a risk analysis. NIST SP 800-30 discusses using “risk models” that examine threats, vulnerabilities, likelihood, and impact. NIST SP 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.

Mitigations may be implemented that can limit a threat event’s likelihood, address or limit asset vulnerabilities, or manage adverse impact. This paper uses the high-level reference architecture that deconstructs the HaH system into components found in four distinct domains as described in Sec. 2. This paper next considers threats and respective risks and recommends contextualized risk mitigations.

In this publication, the NCCoE assumes that components may include vulnerabilities, particularly when using older hardware and software versions. A common mitigation recommendation would entail that HDOs perform appropriate vulnerability or patch management which may pose challenges considering that some HaH components are medical or biometric devices where patches may not be readily available. This paper’s focus highlights other mitigations that reduce threat event likelihood or mitigate adverse impact.

HDOs should also be aware that the evolving threat landscape and advancements in IoT technologies increase vulnerabilities in the HaH ecosystem. HDOs are increasingly relying on third-party providers for HaH and other telehealth solutions which could introduce supply chain risks. HDOs can reference NIST SP 800-161, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* [8] for guidelines. Continuous updates to risk assessments and mitigation strategies are essential to help HDOs protect patient data and critical services.

3.1. Sample Threat Events

As HDOs implement technologies such as HaH or other innovative solutions, they should apply risk assessment guidelines as described in NCCoE practice guides. The NCCoE applied a risk assessment and performed an analysis of the smart home integration ecosystem that identifies several cybersecurity and privacy challenges along with proposed mitigation approaches. The following list shows some example threat events that may cause those cybersecurity and privacy challenges within the smart home 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, healthcare integration solution, and hospital information systems or by exploiting insecure API configurations.
- **Denial of Service (DoS):** An unauthorized actor disrupts the voice assistant communication ecosystem's availability and predictability by flooding the healthcare integration solution platform or hospital information systems with API requests, causing the system to not function as expected. Additionally, a home might have other devices and systems running at the same time which could impact the performance or availability of critical HaH communications (i.e., an unintentional DoS).
- **Operating system (OS) or application disruption:** An unauthorized actor decreases patient data integrity, system availability, and data or system predictability by altering voice commands sent to the healthcare integration solution or altering code running in the healthcare 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 diagram portrays five threat types: 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. It is important to clarify that medical or biometric devices and other personal connected devices within the patient's home are not the primary focus of this analysis, as they were thoroughly addressed in NIST SP 1800-30, *Securing Telehealth Remote Patient Monitoring Ecosystem* [9]. While threats exist to the voice assistant platform and the healthcare integration solution, 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 a 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 the 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.

This paper has identified representative threats within the high-level reference architecture below. 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.

This paper has identified representative threats and proposed mitigation strategies based on NIST Frameworks and IoT publications.

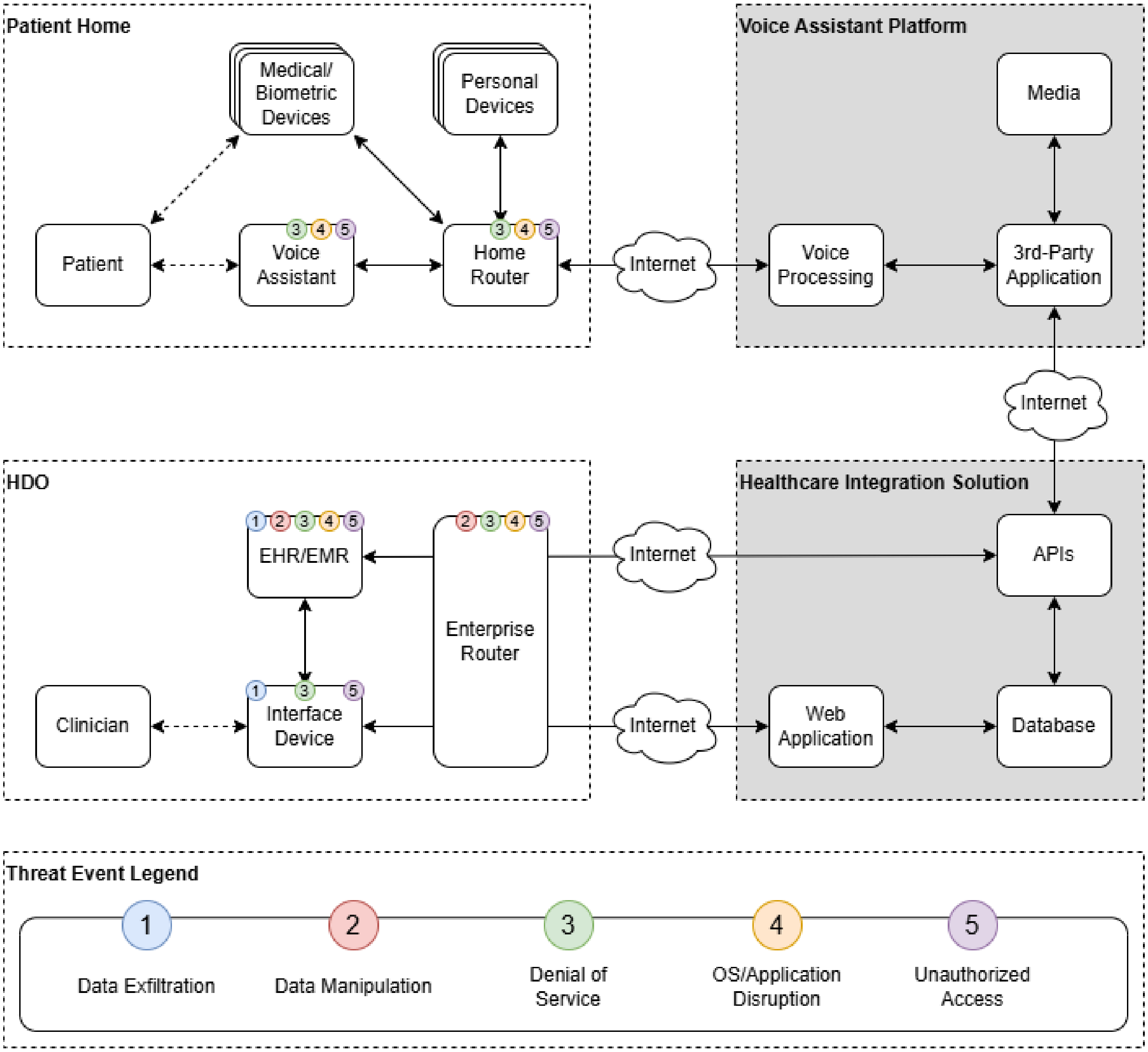

Fig. 2 - High-Level Reference Architecture (with Threat Events)

3.2. Recommended Cybersecurity and Privacy Mitigations

To address the cybersecurity and privacy challenges that arise from these threat events, this paper proposes mitigations aligned with the sample threat events.

This paper applies guidelines from the CSF 2.0 [1], the PF 1.0 [2], and NIST IR 8425 [3]. The recommended mitigations include access control, authentication, continuous monitoring, data security, governance, and network segmentation.

To provide a comprehensive understanding, Table 1 below details how the CSF 2.0, PF 1.0, and NIST IR 8425 can be applied to the recommended mitigations. NIST IR 8425 identifies cybersecurity capabilities expected of consumer IoT products (e.g., voice assistants) and IoT product developers. Selecting IoT products that include these capabilities can help achieve the recommended mitigations.

Table 1: Recommended Cybersecurity and Privacy Mitigations

Recommended Mitigations	Mitigation 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 reduce 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 protect patient data from unauthorized access or alteration and maintains data confidentiality and integrity. [PF Focus] Access control supports the manageability goal by allowing granular administration of PII and the predictability goal by enabling reliable assumptions about PII processing. [NIST IR 8425 Focus] Consumer IoT products (e.g., voice assistant) should 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 aligns with NIST SP 800-207, *Zero Trust Architecture* [10], which enhances security by verifying identities before granting access, thus preventing unauthorized access and safeguarding patient data's integrity and confidentiality. [PF Focus] Authentication supports the predictability goal by ensuring reliable assumptions about who can access PII. [NIST IR 8425 Focus] Consumer IoT products (e.g., voice assistant) should 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 unusual traffic patterns (e.g., indicative of a distributed denial of service [DDoS] attack) and supports the deployment of appropriate mitigation measures, such as traffic filtering, rate limiting or automated blocking mechanisms, to respond effectively. This mitigation 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.

Recommended Mitigations	Mitigation Description
	[PF Focus] This monitoring supports the predictability goal by ensuring the system operates as expected. [NIST IR 8425 Focus] Consumer IoT products (e.g., voice assistant) should 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 that protects sensitive patient data during storage and transmission, maintaining data confidentiality and integrity and preventing unauthorized actors from accessing or altering the data. [PF Focus] This form of security supports the disassociability goal by ensuring PII is processed without association with individuals beyond operational requirements. [NIST IR 8425 Focus] Consumer IoT products (e.g., voice assistant) should 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, and implementing rules and procedures for managing and securing data is 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 is important to have up-to-date documentation and a list of all the systems and API versions being used, which helps avoid problems like outdated API versions and exposed access points. [PF Focus] This governance supports the predictability and manageability goal by allowing granular administration of PII in accordance with the stated purposes of collection. It also ensures that unintentionally collected PII is handled appropriately in accordance with data minimization and retention policies. [NIST IR 8425 Focus] Throughout the development lifecycle, the IoT product developer should create, gather, and store information relevant to the cybersecurity of the IoT product and its product components. Additionally, the IoT product developer should broadcast (e.g., to the public) and distribute (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 medical or biometric 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 segmentation supports the disassociability goal by limiting the association of PII to individuals or devices beyond operational requirements.

Recommended Mitigations	Mitigation Description
	[NIST IR 8425 Focus] Consumer IoT products (e.g., voice assistants) should 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 to change the configuration settings of authorized individuals (i.e., customers), services, and other IoT product components.

3.3. Assess Cybersecurity and Privacy Mitigation Coverage

This paper evaluates the recommended mitigation coverage by applying the NIST CSF 2.0 [1], the PF 1.0 [2], and NIST IR 8425 [3] to the identified threat events in Sec. 3.1. The paper maps the recommended mitigations provided in Sec. 3.2 to CSF 2.0 and PF 1.0 Categories and Subcategories, as well as IoT device capabilities and sub-capabilities from NIST IR 8425.

Both the CSF 2.0 and PF 1.0 share a foundation where they identify Functions, Categories, and Subcategories. The NIST PF 1.0 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. Furthermore, it 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 1.0.

Additionally, this publication lists capabilities from NIST IR 8425 that are applicable to the mitigations provided in Sec. 3.2. NIST IR 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 mitigations identified in Sec. 3.2 and NIST CSF 2.0 [1], PF 1.0 [2], and NIST IR 8425 [3] can be found online in the Assess Cybersecurity and Privacy Mitigation Coverage spreadsheet.

In addition to the recommended mitigations, cybersecurity and privacy awareness and training are essential to address risks in HaH environments. HDOs may implement tailored training programs for HaH staff and patients to help them recognize threats, follow best practices, and protect sensitive health data. Refer to NIST CSF 2.0 [1] and the PF 1.0 [2] for more information on awareness and training.

4. Security Reference Architecture

Figure 3 depicts the high-level reference architecture for a smart home integration ecosystem. This 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 the security and privacy mitigations from Sec. 3.2 to address potential threats. These security and privacy mitigations include access control, authentication, continuous monitoring, data security, governance, and network segmentation.

This paper highlights mitigations that could be implemented in the patient's home and HDO environments. Although safeguarding the voice assistant platform and the health integrator environment is essential, the responsibility for implementing appropriate security and privacy mitigations lies with their respective suppliers. It is important for HDOs to understand how their suppliers and partners address cybersecurity and privacy risks, extending beyond the scope of the issues covered in this paper.

In the patient's home, HDOs may implement security mitigations that include access control, authentication, data security, and network segmentation that provide safeguards for patient interactions with the voice assistant and medical or biometric devices. The patient's home should include network segmentation that separates the HDO-provided medical or biometric devices from the patient's home network. This segmentation may be implemented by placing an HDO-managed router between the medical or biometric devices and the patient's home router. Network segmentation, a concept discussed in NIST SP 1800-30, *Securing Telehealth Remote Patient Monitoring Ecosystem* [9], isolates the medical or biometric devices from potential threats on the patient's home network and helps ensure that HaH components only communicate with authorized services and endpoints. Given the widespread presence of vulnerable devices in home networks, implementing network segmentation is highly recommended in such environments.

Access control and authentication are also important in the patient's home domain. HDO-provided medical or biometric devices should restrict access only to authorized individuals. Medical or 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. The managed router in patient homes could also include a backup connectivity method, such as cellular connectivity, so that connectivity can be maintained even if the home router is subject to a DoS attack.

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 medical data through the voice-enabled application. Finally, this paper recommends implementing data security in the form of data encryption for any communication between the patient's home and other domains.

If HDOs will be deploying managed routers to patient homes, it is recommended that they acquire and deploy routers that conform with the requirements in NIST IR 8425A, *Recommended Cybersecurity Requirements for Consumer-Grade Router Products* [11]. Routers serve as the gatekeepers of our networks that manage 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 alignment with Zero Trust principles as outlined in NIST SP 800-207, *Zero Trust Architecture* [10], this paper emphasizes the implementation of comprehensive security and privacy mitigations within the HDO. These mitigations include access control, authentication, continuous monitoring, data security, and governance, all designed to enforce the “never trust, always verify” approach. These measures are applied across critical components such as the EHR, interface device, and enterprise router/network. Consistent with Zero Trust, any endpoint connected to the HDO network should be authenticated, monitored, and managed using mature inventory and asset management practices to ensure no implicit trust is granted. Sensitive data, whether stored or shared internally or externally, should be protected through encryption to maintain confidentiality and integrity. Furthermore, this paper advocates for strict identity verification and role-based access for HDO workforce members involved in HaH care, ensuring they are authenticated to the devices and systems they use and granted access only to the resources for their specific roles, thereby minimizing the attack surface and adhering to the principle of least privilege.

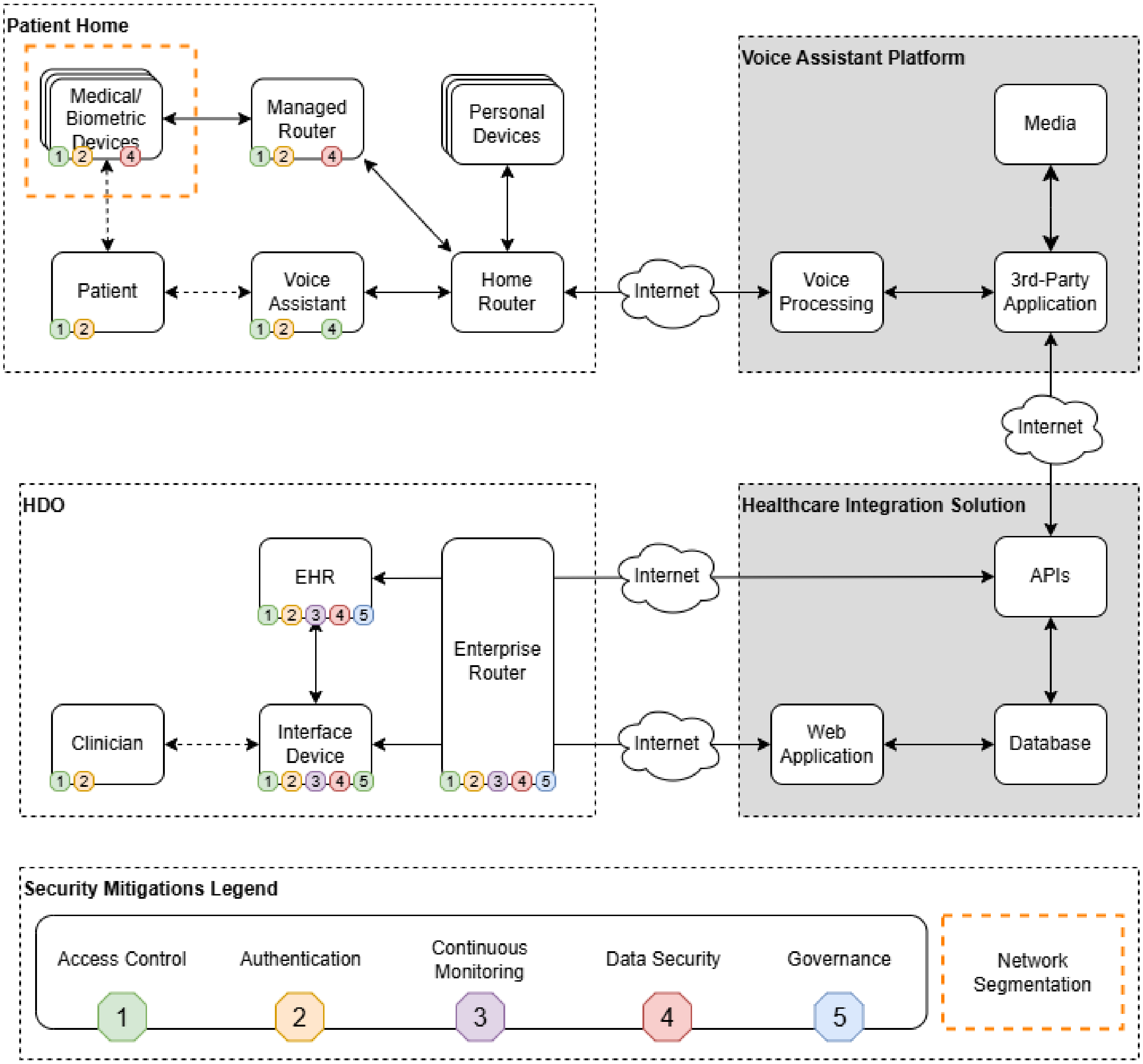

Fig. 3 - High-Level Reference Architecture (with Recommended Mitigations)

5. Conclusion

HaH presents cybersecurity and privacy risks that hospitals must consider [9]. As shown in this paper, HaH and smart home integration involves interconnecting disparate environments not managed directly by the hospital. HDOs depend on third parties to provide application functionality and integration into a hospital's health information system. For example, smart speaker manufacturers may control the endpoint configuration, enabling user interface capabilities by providing the mechanism for NLP and interpreting commands that integrate with application functionality. They may also provide audio interpretation for the patient, enabling an ambient computing experience. Each of these environments offers landscapes that are prone to cyber-attacks and disruption.

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

- 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 potentially unconsidered cybersecurity and privacy threats. This paper has identified representative threats and proposed mitigation strategies based on NIST Frameworks and IoT publications. These mitigations should not be done in siloes or separate from the rest of an organization's cybersecurity strategy and program. Hospitals 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] Fagan M, Megas K, Watrobski P, Marron J, Cuthill B (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 (SP) 800-30 Revision 1, *Guide for Conducting Risk Assessments*. Available at https://doi.org/10.6028/NIST.SP.800-30r1

[8] Boyens J, Smith A, Bartol N, Winkler K, Holbrook A, Fallon M (2024). *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations.* (National Institute of Standards and Technology, Gaithersburg, MD), NIST SP 800-161 Revision 1, Update 1. Available at https://doi.org/10.6028/NIST.SP.800-161r1-upd1

[9] 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. https://doi.org/10.6028/NIST.SP.1800-30

[10] Rose S, Borchert O, Mitchell S, Connelly S (2020). NIST Special Publication 800-207, *Zero Trust Architecture*. Available at https://doi.org/10.6028/NIST.SP.800-207

[11] Fagan M, Megas K, Watrobski P, Marron J, Cuthill B, Lemire D, Hoehn B, Evans C (2024). *Recommended Cybersecurity Requirements for Consumer-Grade Router Products* (National Institute of Standards and Technology, Gaithersburg, MD), Draft NIST Internal Report (NIST IR) 8425A. Available at https://doi.org/10.6028/NIST.IR.8425A

Appendix A. List of Symbols, Abbreviations, and Acronyms

API
Application Programming Interface

CSF 2.0
NIST Cybersecurity Framework 2.0

CSWP
Cybersecurity White Paper

DDoS
Distributed Denial of Service

DoS
Denial of Service

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

NIST IR
NIST Internal Report

NLP
Natural Language Processing

OS
Operating System

PF
NIST Privacy Framework

PII
Personal Identifiable Information

SP
Special Publication

TCP
Transmission Control Protocol