



Check for updates

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

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

5 **NIST Technical Series Policies**

6 [Copyright, Use, and Licensing Statements](#)

7 [NIST Technical Series Publication Identifier Syntax](#)

8 **How to Cite this NIST Technical Series Publication:**

9 Pulivarti R, Littlefield K, Patrick B, Wang S, Williams R (2024) Mitigating Cybersecurity and Privacy Risks in
10 Telehealth Smart Home Integration: Healthcare Sector Risk Management Approaches. (National Institute of
11 Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 34 ipd.
12 <https://doi.org/10.6028/NIST.CSWP.34.ipd>

13 **Author ORCID iDs**

14 Ronald Pulivarti: 0000-0002-8330-3474

15 Kevin Littlefield: 0009-0007-2168-6282

16 Bronwyn Patrick: 0009-0001-7885-4773

17 Sue Wang: 0000-0003-4587-429X

18 Ryan Williams: 0009-0007-5158-309X

19 **Public Comment Period**

20 November 6, 2024 – January 6, 2025

21 **Submit Comments**

22 hit_nccoe@nist.gov

23 National Institute of Standards and Technology

24 Attn: Applied Cybersecurity Division, Information Technology Laboratory

25 100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

26 **Additional Information**

27 Additional information about this publication is available at [Mitigating Cybersecurity Risk in Telehealth Smart](#)

28 [Home Integration](#), including related content, potential updates, and document history.

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

30 **Abstract**

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

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

51 **Keywords**

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

55 **Audience**

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

59 **Note to Reviewers**

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

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

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

73	Table of Contents	
74	Executive Summary	1
75	1. Introduction	2
76	2. Telehealth Smart Home Integration Ecosystem	3
77	3. Smart Home Integration Ecosystem Risk Analysis	4
78	3.1. Sample Threat Events	5
79	3.2. Recommended Cybersecurity and Privacy Practices.....	7
80	3.3. Assess Cybersecurity and Privacy Control Coverage	9
81	4. Security Reference Architecture	10
82	5. Conclusion	12
83	References	14
84	Appendix A. List of Symbols, Abbreviations, and Acronyms	15
85	List of Tables	
86	Table 1: Recommended Cybersecurity and Privacy Practices	8
87	List of Figures	
88	Figure 1 - High-Level Smart Home Integration Reference Architecture	4
89	Figure 2 - High-Level Reference Architecture (with Threat Events)	7
90	Figure 3 - High-Level Reference Architecture (with Recommended Controls)	12

91 **Acknowledgments**

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

97 **Executive Summary**

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

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

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

119 This paper uses NIST guidance in framing risks and proposing mitigating controls. The National
120 Cybersecurity Center of Excellence (NCCoE) healthcare team applies guidance from the
121 *National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0 (CSF 2.0)*
122 [\[1\]](#), the *NIST Privacy Framework (PF)* [\[2\]](#), and *NIST Internal Report (NISTIR) 8425 Profile of the*
123 *IoT Core Baseline for Consumer IoT Products* [\[3\]](#) as well as concepts discussed in previous NCCoE
124 practice guides.

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

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

138 1. Introduction

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

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

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

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

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

178 [\[2\]](#), and *NIST Internal Report (NISTIR) 8425 Profile of the IoT Core Baseline for Consumer IoT*
179 *Products* [\[3\]](#).

180 **2. Telehealth Smart Home Integration Ecosystem**

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

- 186 • Patient Home
- 187 • Voice Assistant Platform
- 188 • Healthcare Integration Solution
- 189 • HDO

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

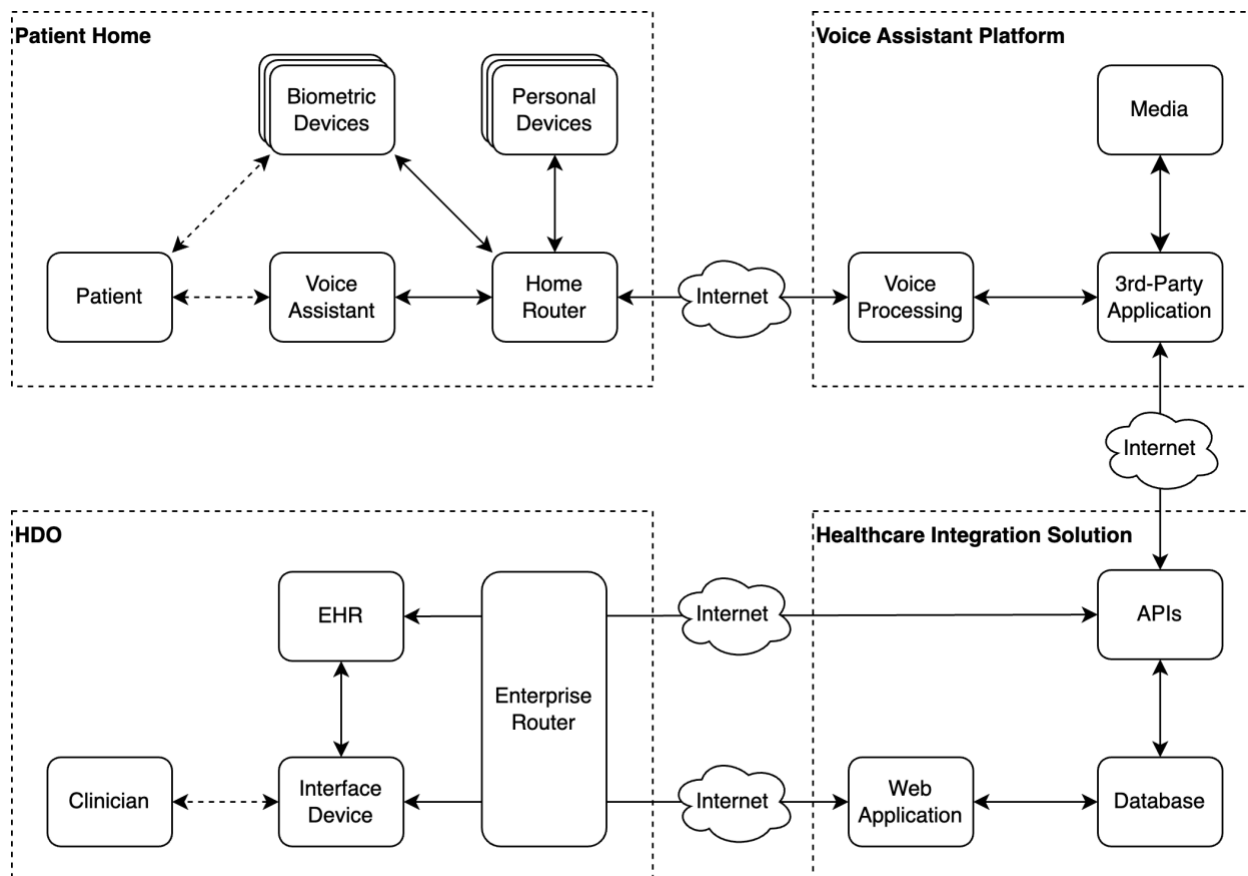
198 The voice assistant platform contains all the backend services that the voice assistant uses to
199 interpret patient commands and perform actions. This includes voice processing services such
200 as NLP (speech-to-text, text-to-speech, etc.) as well as the infrastructure to route the patient's
201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

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

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

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

220 **Figure 1 - High-Level Smart Home Integration Reference Architecture**



221 3. Smart Home Integration Ecosystem Risk Analysis

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

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

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

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

245 **3.1. Sample Threat Events**

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

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

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

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

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

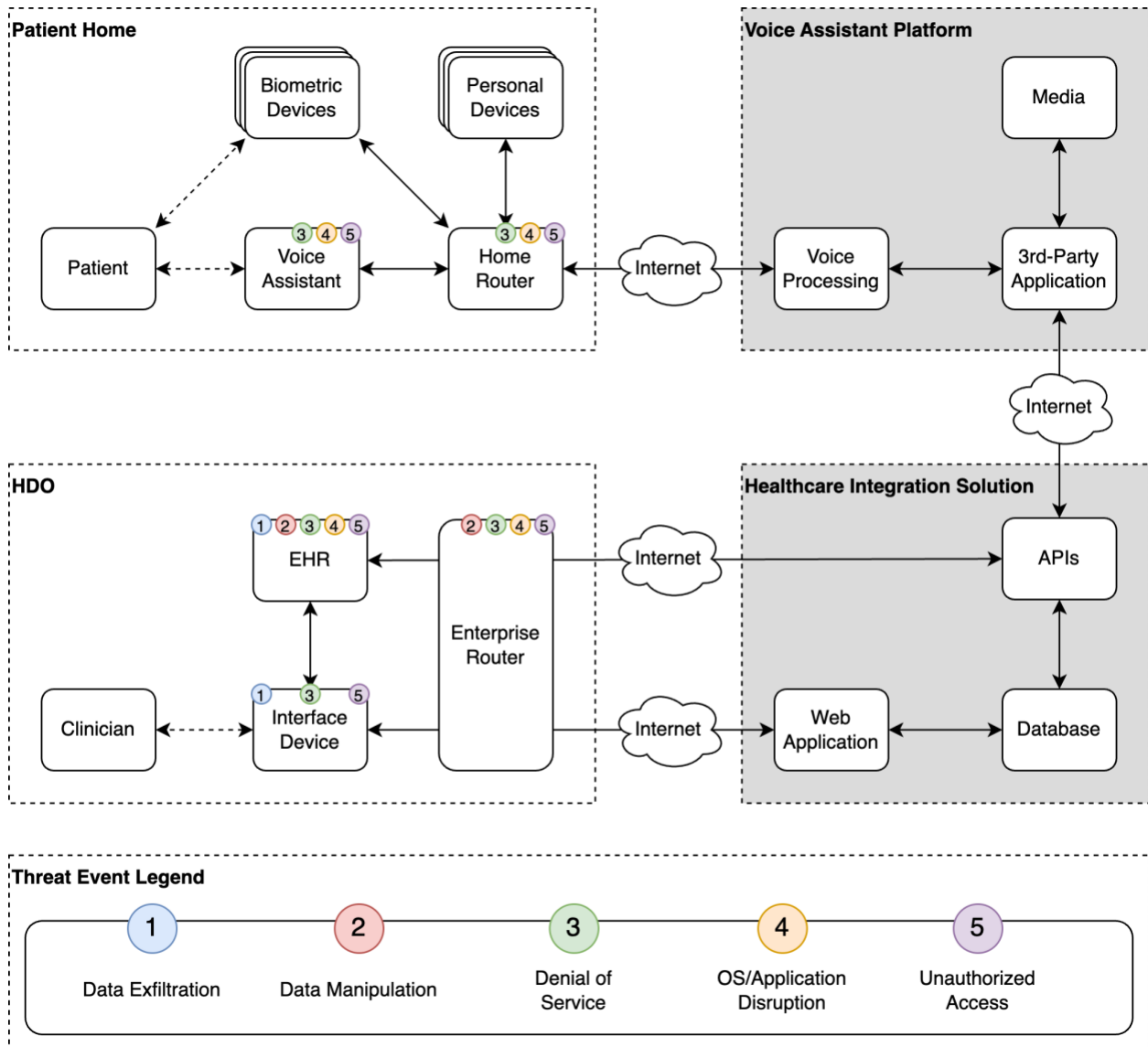
280 In the patient's home domain, the voice assistant may be prone to denial of service,
281 OS/application disruption, or unauthorized access. The diagram also depicts a home router
282 component that would operate as the home network's backbone and means to connect to the
283 internet. The home router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

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

291 The threats discussed in this paper are representative. HDOs implementing HaH solutions may
292 identify different threats and expand on the threat types and components that may be affected
293 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	<p>[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.</p> <p>[PF Focus] This supports the manageability goal by allowing granular administration of PII and the predictability goal by enabling reliable assumptions about PII processing.</p> <p>[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.</p>
Authentication	<p>[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.</p> <p>[PF Focus] This supports the predictability goal by ensuring reliable assumptions about who can access PII.</p> <p>[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.</p>
Continuous Monitoring	<p>[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.</p> <p>[PF Focus] This supports the predictability goal by ensuring the system operates as expected.</p> <p>[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.</p>
Data Security	<p>[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</p>

Recommended Control	Control Description
	<p>confidentiality and integrity and preventing unauthorized actors from accessing or altering the data.</p> <p>[PF Focus] This supports the disassociability goal by ensuring PII is processed without association with individuals beyond operational requirements.</p> <p>[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.</p>
Governance	<p>[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.</p> <p>[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.</p> <p>[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.</p>
Network Segmentation	<p>[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.</p> <p>[PF Focus] This supports the disassociability goal by limiting the association of PII to individuals or devices beyond operational requirements.</p> <p>[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.</p>

305 **3.3. Assess Cybersecurity and Privacy Control Coverage**

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

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

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

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

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

326 **4. Security Reference Architecture**

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

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

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

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

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

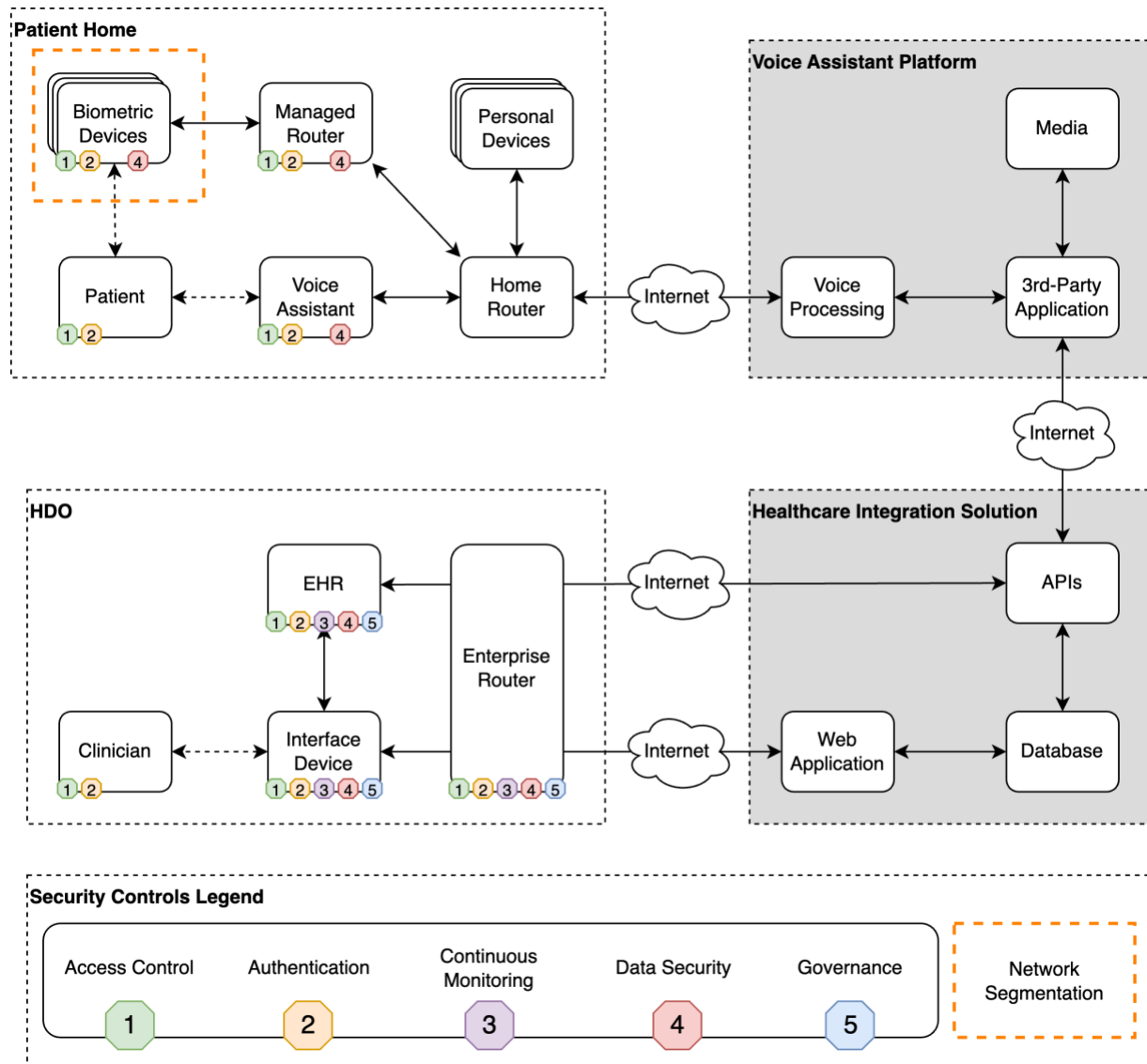
357 Security concepts should also apply to the voice-enabled application the patient interacts with,
358 through their voice assistant, to communicate with the HDO. While it is not reasonable to
359 physically segment the patient-owned voice assistant from the home network, HDOs should
360 ensure that only the patient can access their own medical data through the voice-enabled
361 application. Finally, this paper recommends implementing data security controls in the form of
362 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.

363 In the HDO, this paper recommends comprehensive security and privacy controls. A
364 comprehensive control set includes access control, authentication, continuous monitoring, data
365 security, and governance. All five controls have been applied to the EHR, interface device, and
366 enterprise router/network. Any endpoint connected to the HDO network should be
367 authenticated, monitored, and managed using mature inventory and asset management
368 practices. Sensitive data stored or shared internally or externally should be secured through
369 encryption. This paper also recommends that the HDO workforce members associated with
370 providing HaH care be properly authenticated to the devices and systems they use and only
371 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.

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

- 387 • Data exfiltration
- 388 • Data manipulation
- 389 • Denial of service
- 390 • Operating system or application disruption
- 391 • Unauthorized access

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

- 396 • Access control
- 397 • Authentication
- 398 • Continuous monitoring
- 399 • Data security
- 400 • Governance
- 401 • Network segmentation

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

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

416 **References**

- 417 [1] National Institute of Standards and Technology (2024) *The NIST Cybersecurity Framework*
418 *(CSF) 2.0*. Available at <https://doi.org/10.6028/NIST.CSWP.29>
- 419 [2] National Institute of Standards and Technology (2021) *NIST Privacy Framework: A Tool for*
420 *Improving Privacy Through Enterprise Risk Management, Version 1.0*. Available at
421 <https://doi.org/10.6028/NIST.CSWP.01162020>
- 422 [3] Michael F, Katerina M, Paul W, Jeffrey M, Barbara C (2022). *Profile of the IoT Core Baseline*
423 *for Consumer IoT Products* (National Institute of Standards and Technology, Gaithersburg,
424 MD), NIST Internal Report (NIST IR) 8425. Available at
425 <https://doi.org/10.6028/NIST.IR.8425>
- 426 [4] American Hospital Association (2020) *The Value Initiative Issue Brief Creating Value by*
427 *Bringing Hospital Care Home*. Available at
428 [https://www.aha.org/system/files/media/file/2020/12/issue-brief-creating-value-by-](https://www.aha.org/system/files/media/file/2020/12/issue-brief-creating-value-by-bringing-hospital-care-home_0.pdf)
429 [bringing-hospital-care-home_0.pdf](https://www.aha.org/system/files/media/file/2020/12/issue-brief-creating-value-by-bringing-hospital-care-home_0.pdf)
- 430 [5] Food and Drug Administration (2024) *FDA Launches Health Care at Home Initiative to Help*
431 *Advance Health Equity*. Available at [https://www.fda.gov/medical-devices/medical-](https://www.fda.gov/medical-devices/medical-devices-news-and-events/fda-launches-health-care-home-initiative-help-advance-health-equity)
432 [devices-news-and-events/fda-launches-health-care-home-initiative-help-advance-health-](https://www.fda.gov/medical-devices/medical-devices-news-and-events/fda-launches-health-care-home-initiative-help-advance-health-equity)
433 [equity](https://www.fda.gov/medical-devices/medical-devices-news-and-events/fda-launches-health-care-home-initiative-help-advance-health-equity)
- 434 [6] Medicare.gov *Home health services*. Available at [https://www.medicare.gov/what-](https://www.medicare.gov/what-medicare-covers/whats-home-health-care)
435 [medicare-covers/whats-home-health-care](https://www.medicare.gov/what-medicare-covers/whats-home-health-care)
- 436 [7] National Institute of Standards and Technology (2012). NIST Special Publication 800-30
437 Revision 1, *Guide for Conducting Risk Assessments*. Available at
438 <https://doi.org/10.6028/NIST.SP.800-30r1>
- 439 [8] Cawthra J, Grayson N, Pulivarti R, Hodges B, Kuruvilla J, Littlefield K, Snyder J, Wang S,
440 Williams R, Zheng K (2022) *Securing telehealth remote patient monitoring ecosystem*.
441 (National Institute of Standards and Technology (U.S.), Gaithersburg, MD), NIST SP 1800-
442 30, p NIST SP 1800-30. <https://doi.org/10.6028/NIST.SP.1800-30>
- 443 [9] Michael F, Katerina M, Paul W, Jeffrey M, Barbara C, David L, Brad H, Chris E (2024).
444 *Recommended Cybersecurity Requirements for Consumer-Grade Router Products* (National
445 Institute of Standards and Technology, Gaithersburg, MD), Draft NIST Internal Report (NIST
446 IR) 8425A ipd. Available at
447 <https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8425A.ipd.pdf>

448 **Appendix A. List of Symbols, Abbreviations, and Acronyms**

449 **API**

450 Application Programming Interface

451 **CSF 2.0**

452 NIST Cybersecurity Framework 2.0

453 **CSWP**

454 Cybersecurity White Paper

455 **EHR**

456 Electronic Health Record

457 **HaH**

458 Hospital-at-Home

459 **HDO**

460 Healthcare Delivery Organization

461 **IoT**

462 Internet of Things

463 **NCCoE**

464 National Cybersecurity Center of Excellence

465 **NIST**

466 National Institute of Standards and Technology

467 **NISTIR**

468 NIST Internal Report

469 **NLP**

470 Natural Language Processing

471 **OS**

472 Operating System

473 **PF**

474 NIST Privacy Framework

475 **PII**

476 Personal Identifiable Information

477 **SHI**

478 Smart Home Integration

479 **SP**

480 Special Publication

481 **TCP**

482 Transmission Control Protocol