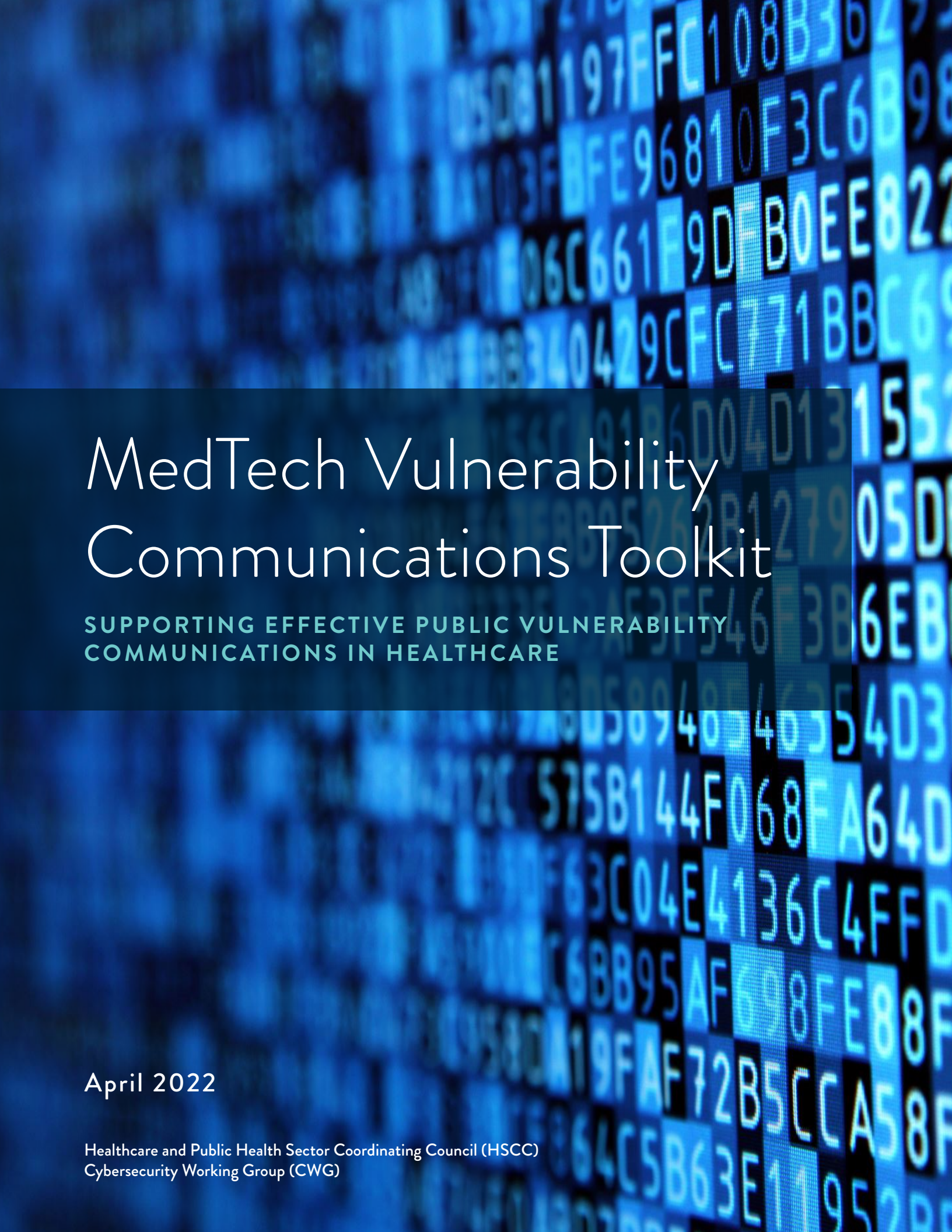

MedTech Vulnerability Communications Toolkit

SUPPORTING EFFECTIVE PUBLIC VULNERABILITY COMMUNICATIONS IN HEALTHCARE

April 2022

Healthcare and Public Health Sector Coordinating Council (HSCC)
Cybersecurity Working Group (CWG)

Table of Contents

Introduction 3

About the Health Sector Coordinating Council 4

Acknowledgments 4

Using This Toolkit 5

Vulnerability Communications Overview 5

Vulnerability Categorization 6

Vulnerability Communications Prioritization Table 7

Glossary of Terms 9

Security Terms 9

Security Threats 11

Healthcare Terms 12

Technology Terms 13

Privacy and Personal Information Terms 13

Government, Research and Security Information-Sharing Terms 15

Terms to Avoid 15

Appendix: Vulnerability Communication Sample Template 17

Introduction

Medical devices are prolific in healthcare environments and increasingly interact directly with patients. An American Hospital Association survey notes that a patient bed has an average of 15 medical devices. Therefore, a 500-bed hospital could have 7,500 devices supporting delivery of healthcare services. In addition, millions of patients use implanted or wearable devices to support monitoring of healthcare vitals or even delivering therapy. Whether used in a hospital or by a patient, medical devices are increasingly connected to enable efficient and cost-effective management of care and access to data to improve healthcare outcomes, both individually and for entire patient populations.

As with any connected technology, increased connectivity is accompanied by new risks, including cybersecurity risks. It is not possible to completely predict and prevent all cybersecurity vulnerabilities, which are often discovered in software and hardware after devices are in use. In healthcare technology, these vulnerabilities can lead to the breach of sensitive information and the potential to cause patient harm. Transparency, effective communication of vulnerabilities and appropriate mitigation strategies are essential to ensure unacceptable risks are adequately managed.

Vulnerability communications have historically been very technical in nature and intended to inform technology and security professionals of risks and recommended actions to mitigate those risks. Healthcare stakeholders don't always possess the experience and knowledge to translate technical information to effectively inform patients and clinicians of potential risks and necessary actions. In October 2021, the FDA published "Best Practices for Communicating Cybersecurity Vulnerabilities to Patients,"[1] which provided essential guidance to improve communication of cybersecurity vulnerabilities to patients.

The Health Sector Coordinating Council (HSCC) Cybersecurity Working Group (CWG) built on the FDA's guidance by forming a Vulnerability Communications Task Group to further improve cybersecurity communication to patients. The task group informed its work by initially surveying healthcare professionals, journalists covering healthcare cybersecurity, security researchers, manufacturers and regulators to determine best practices for communicating to patients. Using this feedback, the task group developed this toolkit to support effective vulnerability communications processes and improve the clarity of messaging to nontechnical audiences, such as patients and healthcare professionals. The HSCC Vulnerability Communications Task Group will continue to research and develop additional resources to support the effective management of risk from medical device vulnerabilities throughout the healthcare ecosystem.

This document is a toolkit written to provide specific tools to medical device manufacturers and software developers for creating cybersecurity vulnerability communications related to their products or services. This toolkit focuses on vulnerability communications directed to nonsecurity professionals, including clinicians, patients, users and other readers not familiar with cybersecurity and connected technologies. It is intended to help medical device manufacturers formulate and communicate vulnerability disclosures that all affected audiences, including nontechnical stakeholders, can understand.

Future versions will focus on more technically oriented audiences in biomedical engineering and cybersecurity roles.

[1]Best Practices for Communicating Cybersecurity Vulnerabilities to Patients. https://www.fda.gov/media/152608/download.

About the Health Sector Coordinating Council

The Healthcare and Public Health Sector Coordinating Council (HSCC) is a coalition of private-sector critical healthcare infrastructure entities organized under the National Infrastructure Protection Plan to partner with and advise the government on the identification and mitigation of strategic threats and vulnerabilities facing the sector's ability to deliver services and assets to the public. The HSCC Cybersecurity Working Group (CWG) is a standing working group of the HSCC, composed of more than 300 industry and government organizations working together to develop strategies to address emerging and ongoing cybersecurity challenges to the health sector.

Acknowledgments

The following individuals constitute the membership of the Vulnerability Communications Task Group committee, established in January 2020, and were responsible for development of the Vulnerability Communications Toolkit and Glossary.

- Task Group Co-Chair Abhishek Agarwal, Chief Information Security Officer, Fresenius Medical Care
- Task Group Co-Chair Chris Tyberg, Divisional Vice President, Product Security, Abbott
- Task Group Co-Chair Jessica Wilkerson, J.D., Senior Cyber Policy Advisor, Center for Devices and Radiological Health, FDA
- Vulnerability Toolkit Task Group Workstream Lead Matt Russo, Senior Director, Product Security, Medtronic
- Glossary Task Group Workstream Leads Laura Robb Élan, Associate Director, Digital Health, Software and Cybersecurity, Baxter Healthcare, and Chris Reed, Director, Regulatory Policy, Medtronic
- Ashley Bellus, Senior Manager, Product Security, Smith & Nephew
- Uma Chandrashekhar, Global Product Security Information Officer, Alcon
- Iain Deason, IT Security Specialist, CISA
- Andrea Sharp, Staff Product Security Analyst, GE Healthcare
- Chad Waters, Senior Cybersecurity Engineer, ECRI
- Kimberly Ann Bauer, Product Security, Eli Lilly and Company
- Linda Hillen, Senior Analyst, Product Security, Abbott
- Judd Larson, Principal Product Security Technologist, Medtronic
- Nastassia Tamari, Director, Information Security Operations, BD (Becton, Dickinson and Company)
- Varun Verma, Global Manager, Regulations and Standards, Philips Healthcare
- Erika Winkels, Director, Corporate Communications, Medtronic
- Jennifer Wolf, Associate Director, Cybersecurity Communication, BD (Becton, Dickinson and Company)
- Mike Powers, Director, Clinical Engineering, Intermountain Healthcare

Using This Toolkit

What's Included in This Toolkit?

This kit provides guidance for publicly disclosing vulnerabilities in medical devices, with a focus on communicating to patients. The kit includes the following:

- **Vulnerability Categorization**
  - Categorization of vulnerabilities helps identify and prioritize the proper healthcare stakeholders to focus on, based on the type of vulnerability.
  - Keeping the target stakeholders in focus prioritizes those who should act while others who require information are adequately considered.
- **Vulnerability Communications Prioritization Table**
  - A guide for what information to collect and prioritize in a vulnerability communication
- **Glossary of Terms**
  - Terms to leverage in vulnerability communications to convey security concepts in healthcare without assuming an excessive background or experience in healthcare security
  - Terms that should not be used; included to guide communications so they are accessible to laypeople (those without professional or specialized knowledge of security)
- **Vulnerability Communication Sample Template**
  - A sample mockup for developing vulnerability communications

Vulnerability Communications Overview

Communicating cybersecurity vulnerability information is complex. It can be even more difficult when communicating to stakeholders who may not be familiar with technical terminology or understand the balance between the cybersecurity risks and health benefits of medical devices. Ensuring that the right information is delivered to the right stakeholders at the right time is critical to successfully mitigating cybersecurity risks. The following high-level process overview identifies the key steps for developing a medical device vulnerability communication and shows how to leverage other resources in this document.

Step 1 Categorize the vulnerability to ensure proper prioritization and consideration for target stakeholders who will need to understand and take action based on the vulnerability communication. Leverage the **Vulnerability Communications Prioritization Table** to collect necessary information to support an effective vulnerability communication.

Step 2 Draft the vulnerability communication based on information captured in the Vulnerability Communications Prioritization Table. The **Vulnerability Communication Sample Template,** included as an appendix, may be leveraged if your organization does not have a template.

Be direct and to the point. Avoid corporate boilerplate content, and use concise, simple language wherever possible:

- A security bulletin should be targeted to a general audience, not a security expert. Consider the specific stakeholder who must take action or would require the information as identified in the vulnerability categorization.
- Leverage the **Glossary of Terms** in this document for support, for both terms to use and terms to avoid. When terms are utilized, it is advised that the definitions should be included to ensure clarity.
- If needed, consider additional, more technical materials aimed at specific audiences (e.g., hospital IT professionals).

Step 3 Partner with your Communications teams for reviews and to refine and ensure the language and format are appropriate for your organization.

Vulnerability Categorization

The following graphic may be used to assist in categorizing a vulnerability and prioritizing the stakeholder communication. Prioritization, in the context of the table below, is not focused on communication order but on identifying the primary audience(s). This helps ensure that the communication best meets the needs of the intended audience, those who need it most to guarantee a vulnerability response.

Medical Device Cybersecurity Communication Style Categories

Category 0 Widely publicized vulnerabilities that **do not** impact a medical device manufacturer's products	**Category 1** Manufacturer-controlled apps and cloud services (not patient-facing)	**Category 2** Devices for which an HDO representative is the primary user **Examples:** capital equipment, computer-on-wheels form factors	**Category 3** Devices for which the patient is the primary user **Example:** pacemaker **Category 3+ Technical** Devices with more involved patients **Example:** insulin pump
Stakeholders may appreciate knowing that a manufacturer is aware, but there is no value added. Communication may be targeted to a general audience.	The manufacturer is responsible for the fix.	The manufacturer is reliant on the HDO to apply the fix or grant access for it to be applied.	The manufacturer is reliant on patients or clinicians to apply the fix or grant access for it to be applied.
	Stakeholder priority 1. HDO biomed/IT 2. Clinicians 3. Patients 4. Regulators	Stakeholder priority 1. HDO biomed/IT 2. Clinicians 3. Patients 4. Regulators	Stakeholder priority 1. Patients 2. Clinicians 3. HDO biomed/IT 4. Regulators

This sheet is intended to help medical device manufacturers focus and prioritize their communication styles for the stakeholders most relevant to the security issue being disclosed.

Type of device **Characterization of who needs to take action** **Recommended stakeholder prioritization**

Figure 1: Categorization of Vulnerabilities

Vulnerability Communications Prioritization Table

The following table provides guidance for what information to collect, include and prioritize in a vulnerability communication, with more important content appearing earlier in the disclosure. (The content of this guide is prioritized in the order in which it appears in the table below, with the most important content toward the top.)

Questions to Be Answered	Guidance Details	Content to Be Populated by Medical Device Manufacturer
Note: If the answer is **no** or **not applicable** to any of these questions, the corresponding information may be omitted from the formal vulnerability communication.		
Is this an update to a prior bulletin?	Include the initial date of publication and a complete history of revisions.	
What device is impacted?	Include information to identify the impacted device(s), as appropriate. (This may include an entire device line or family, if applicable.): • Images of the device • Brief device description • Model name • Model number(s) • Version • Unique device identifier (UDI) • Software versions affected • Any other information that may help the user identify the impacted device(s) ***Note: Graphics, formatting and information layout considerations are useful for visual identification of the device and ease of readability or understanding of the vulnerability.***	
How does this impact care delivery?	A cybersecurity bulletin is meant to inform, so that stakeholders responsible for care can weigh this information against other risks.	
What is the vulnerability?		
What is the risk associated with the vulnerability?	The explanation for a cybersecurity vulnerability communication should include focused risks for the following: • Patients • Doctors • Health delivery organization (HDO) or biomedical engineering • Other relevant stakeholder(s) If appropriate, content may be duplicative to best communicate to different audiences. The choice of which audiences to address directly depends on the type of device, its intended use and the type of vulnerability. Refer to the "Communication Categories" document included in this kit for further guidance.	

Table continued on the next page. →

Vulnerability Communications Prioritization Table (cont.)

Questions to Be Answered	Guidance Details	Content to Be Populated by Medical Device Manufacturer
What actions are you taking to address the risk?	Actions should include any activities the medical device manufacturer has complete control over.	
What actions can a user of the device perform?	Compensating controls or recommendations should be included, such as industry best practices for cybersecurity (e.g., network segmentation, physical controls).	
What is the relevant contact information?	Contact information should include support departments for both technical customer support and a nontechnical contact, if feasible. Ensure that contact information is global and not market- or region-specific.	
What other relevant information should be included? (Not all information is required. The medical device manufacturer should provide as much information as possible to provide clarity on the fix/mitigation.)	Other relevant information to consider: • Security researcher or vendor who reported the vulnerability • Timeline • Mitigation of similar risks • System/network diagrams • Videos • CVSS score • CVE	

Glossary of Terms

It is not the intent of this glossary to redefine the terms included herein. Rather, it provides explanations for common security terms that may be used in vulnerability communications, so they are accessible and understandable to laypeople (those without professional or specialized knowledge in security). For the purposes of this document, a layperson is considered an average person in the United States, with a grade level at or below the high school level and no specialty training in technology.

In addition to explaining common terms, this document makes recommendations about terms to avoid when crafting communications for readers who may not be familiar with security terminology, technology or methods.

The security terms are grouped into six sections:

- Security Terms
- Security Threats
- Healthcare Terms
- Technology Terms
- Privacy Concepts
- Government, Research and Security Information-Sharing Terms

Security Terms

Security terms are general terms that apply across all devices and software development organizations. They provide a road map for different methods and processes that an organization, entity or person may take to protect information, devices and systems. These terms are common across organizations and manufacturers, and they describe specific goals, risks and methods related to security.

Advisory – An advisory is a communication that provides information about a security issue related to a specific product or service. Information should contain a description of the security issue, including guidance on the level of risk and recommended actions for the intended audience of the notification. The communication may take the form of an email message, text message, website or physical document sent to specific users of a product or service. An advisory is also known as a bulletin or vulnerability note.

Alert – An alert is a notification regarding current time-sensitive vulnerabilities, exploits and other security issues. Typically, this is to notify the intended audience of any unusual activity, danger, threat or problem to enable the intended audience to effectively avoid or deal with the issue. An alert may reference a related advisory that provides more detailed information to allow the intended audience to take appropriate action.

Authentication – Authentication is the process of recognizing and affirming a user's identity. Authentication typically uses specific information about a user, such as something only the user knows (password, security question), a physical characteristic (fingerprint, facial recognition), or something they have (email address, mobile phone number). Multifactor authentication includes more than one type of information to confirm a person's identity. For example, a banking website may ask a user to enter their username and password (something they know) and then send an email or text message (something they have) with a temporary code number that allows the completion of the activity or action.

Authorization – In computer security, authorization is the process of giving the user permission to access specific products, files, data or information. For example, when a user enters their username and password, the security system then determines what types of activities or information the user can access. In most cases, authorization is limited to only the functions or data necessary for the user to perform the interactions they need.

continued →

Security Terms (cont.)

Availability – In computer security, availability means that a product or software system is operational at a given time.

Confidentiality/confidential – In computer security, confidentiality is a property of information and data that means it should only be disclosed or shared with users of that product or system who have permission to read, change or in other ways interact with the information or data. In healthcare systems, confidential information is considered private information of a person or an entity. Confidential information may include an individual's personal identity information, such as name, age, address or insurance information, as well as information about their health and healthcare, such as health conditions or medications.

Controlled risk – The U.S. FDA has defined controlled risk in its cybersecurity guidance as "when there is sufficiently low (acceptable) residual risk of patient harm due to the vulnerability." A controlled risk occurs when a cybersecurity weakness or vulnerability is found in a product or system and where the security risk is unlikely to affect safe operation of the product or system because there are enough security controls to protect safety. The decision for assessing controls versus risk is determined by the product's manufacturer.

Cybersecurity – Cybersecurity is the practice of protecting against criminal or unauthorized use of electronic data. It is often associated with a physical or real-world harm, such as injury to a person or financial loss to a person or an organization. Cybersecurity is often called security or information security.

Encryption – Encryption is the process of modifying data or information so it is not recognizable or readable by a human. Encryption is performed using predefined calculations, called algorithms, that have a key. To change the data back from its encrypted form to its readable form, a person must have the key and know the specific algorithm used. Encryption keeps private and sensitive data safe from being read by someone who does not have permission to read or use it.

Exploitability – Exploitability describes how easily a security vulnerability can be used to achieve a desired outcome, such as stealing information or destroying computer systems or their ability to perform intended functions. Not all security vulnerabilities are easy to exploit. Therefore, product manufacturers, systems owners and/or security researchers often evaluate how easy it is to compromise a system using an identified exploit and then plan an appropriate response, such as a countermeasure or vulnerability communication. (Also, see **Exploit** under **Security Threats**.)

Information security – Information security is the practice of protecting information in physical or electronic forms against unauthorized use or abuse and/or catastrophic events, such as natural disasters. Information security is often called security or cybersecurity.

Integrity – Integrity refers to the assurance that data used in or transmitted by a system or device is maintained in its original state and is only changed by people who have permission to ensure the data is accurate and can be trusted.

Retention – Retention is the amount of time information is stored in a computer system.

Security patch – A patch is basically a repair job for a piece of software programming. A security patch provides a solution to an identified problem, such as a new cybersecurity weakness or outdated component. It is primarily provided to fix, update or improve a system.

continued →

Security Terms (cont.)

Security researcher – A security researcher is someone who uses deep technical knowledge of the way medical devices and computer systems process information to identify new vulnerabilities. A security researcher may find a weakness in any form of technology, from the way a specific encryption protocol sends and receives information to a more high-level weakness, like a website with sensitive data that should not have been made available to the public. Some security researchers work in an academic environment, in which they identify such weaknesses for the purpose of sharing the information with a broad audience. Others may be interested in identifying weaknesses, so they can collaboratively share the information with entities who can fix them. (These researchers are sometimes referred to as ethical hackers or white hat hackers because their efforts are intended to inform or protect the security of systems instead of causing harm.) Still other security researchers identify weaknesses to either exploit the weakness for their own malicious intents or to share them with others who will maliciously exploit the weakness. (These researchers are sometimes called black hat hackers.)

Uncontrolled risk – The U.S. FDA has defined uncontrolled risk in its cybersecurity guidance as where "there is unacceptable residual risk of patient harm due to inadequate compensating controls and risk mitigations." An uncontrolled risk occurs when a cybersecurity weakness or vulnerability is found in a product or system and where the security risk is likely to affect safe operation of the product or system because there are not enough security controls to protect safety. The decision for assessing controls versus risk is determined by the product's manufacturer.

Security Threats

A security threat is any one of a number of things that can damage computer systems or the data that resides in computer and network systems. There are different kinds of threats, but the most common are actions performed by cybersecurity criminals. Some threats include breaking into computer systems or networks by guessing, or cracking, the system's security, such as passwords. Another type includes malicious software, or malware, that can be loaded onto computer systems or networks, often via emails with embedded links, to perform many types of damaging effects. Security threats also include natural disasters, such as hurricanes, tornados, earthquakes and fires that can destroy buildings or equipment that supports computer systems or networks.

In essence, any action or condition that has the ability to steal information, break equipment, destroy data or information, or cause computer systems and networks to operate in a nonprescribed way can be considered a security threat. This section of the glossary describes several common security threats.

Data breach – A data breach is an event in which private or confidential information is exposed, stolen or destroyed by a person or entity that did not have permission to access, change or remove that information. One example of a data breach is when a cybercriminal accessed the customer information database managed by cellular company T-Mobile and copied customer data, including names, birthdates, credit card information and Social Security numbers.

Denial of service (DoS) – A DoS is a type of cyberattack that is meant to shut down a machine, function or network, making it inaccessible to its intended users by consuming available resources with invalid activity. The most common DoS technique is to send invalid network requests that consume available network resources of an online service.

continued →

Security Threats (cont.)

Exploit – An exploit is a program or methodology created to take advantage of a vulnerability in a system or product to gain unauthorized access or negatively affect proper operation.

Malware – Malware is short for malicious software. Malicious software can be a computer virus or other type of software code used to steal information, destroy data or make systems unusable. Cybercriminals often use malware as a tool to achieve those goals.

Phishing – Phishing is a technique used to trick people into providing sensitive data, like credit card or login information. It is also a way to deceive people into taking actions that will install malware on their computers or mobile devices, such as viewing a malicious web page or opening an attachment.

Ransomware – Ransomware is a type of malicious software or computer virus that scrambles and/or locks up computer data so that it is unusable by the data owner. Often, cybercriminals who use ransomware will then attempt to extort money from the victim in exchange for returning access to the data.

Vulnerability – A vulnerability is a weakness in systems, software or products that compromises security. A vulnerability allows people to perform bad actions on those same systems, software and products.

Worm – A computer worm is a type of malicious software, also called malware, that infects a computer or a computer network. Once it saves itself in the computer system's memory or the network's hardware, it begins to make copies of its own software program. These copies are moved to other parts of the computer system or network, causing a large malware infection. Sometimes, worms have software that damages the system, but many worms do not attack the system directly. By continuing to make copies of themselves, they simply use up all the memory or network resources and crash the computer system.

Healthcare Terms

Healthcare terms are terms that relate specifically to data, records, people or systems used in healthcare settings. Often, healthcare organizations are involved with vulnerability communications, either as the target of the security incident or by taking action to mitigate the result of the security incident.

Electronic health record (EHR) – An EHR is a digital record of healthcare information generated within a medical institution or environment, such as a hospital, clinic or doctor's office. It may include medical history, laboratory results, immunizations, prescription lists and demographics. An EHR is also called an electronic medical record, or EMR.

Healthcare provider – A healthcare provider is any person or organization that furnishes healthcare services and supplies, bills for them, or is paid for them. Healthcare providers can be individuals (doctors, nurses, pharmacists, lab technicians) or organizations (hospitals, clinics, practice groups, along with their administrative staff). Healthcare researchers are also considered providers.

HIPAA – The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a U.S. federal law that created national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge.

Technology Terms

It is often necessary to include terms that describe information technology equipment, software components or specific methods when describing how vulnerabilities have affected security and privacy. Technology terms may be unfamiliar to system users who do not have knowledge of computing hardware, software or security methods.

This section provides explanations of technical terms commonly found in vulnerability communications. It is not our goal to define or redefine these terms. Rather, we mean to provide information that explains each term and offers real-world examples that clarify the use of these terms in vulnerability communications.

Application – An application, or app, is a software or technology tool designed to help someone perform a specific activity. Examples of apps include fitness trackers, word processing programs, photo editing programs and mobile phone navigation programs.

Cloud computing – In a computer system, cloud computing is the practice of using a network of remote servers connected via the internet to store, manage and process data, rather than using a local computer server or personal computer.

Internet protocol (IP) address – A unique series of numbers separated by periods that identifies a device on a computer network. Every device (including computers, mobile phones and medical devices) that communicates on a network or on the internet has a unique IP address. An example of an IP address is 172.16.10.254.

Uniform resource locator (URL) – URL is an acronym that stands for uniform resource locator. A URL is a unique address on the internet. Examples of common URLs are https://www.google.com, https://www.fda.gov, http://healthsectorcouncil.org and http://yale.edu.

Privacy and Personal Information Terms

There are many terms used to describe the concept of privacy or personal information. Simply put, any information that allows someone to infer or know someone else's identity, directly or indirectly, without that person's consent may be in violation of regulations and subject to penalties. An example of a violation is disclosing a patient's health, healthcare or treatment, or any billing and payment related to that treatment, without the patient's consent.

Electronic protected health information (ePHI) – An ePHI is any PHI that is maintained or transmitted in an electronic format, such as in an electronic health record (EHR) or electronic medical record (EMR).

Personally identifiable information (PII) – PII is a general term describing any form of sensitive data that could be used to identify or contact an individual, including Social Security number, phone numbers, mail or email addresses, login IDs, digital images, IP addresses, social media posts, and other digital forms of data. PII is a superset of protected health information. (See definition below.)

Privacy policy – A privacy policy is a policy that defines and governs how an entity, such as a hospital or doctor's office, handles the personal information of its employees and clients. The policy often includes rules about who in the organization is allowed to read, modify or transmit data, based on local laws and the permission of the data owner. In addition, the privacy policy defines the specific rights of each data owner regarding how the data owner's information may be used or to whom it may be communicated.

continued →

Privacy and Personal Information Terms (cont.)

Protected health information (PHI) – Under the U.S. HIPAA privacy rule, PHI (or in the case of electronic health information, ePHI) is any individually identifiable health information held by a covered entity, such as a healthcare provider or health plan, or its business associates. PHI includes these 18 identifiers, as well as any other characteristics that could uniquely identify an individual:

- Name
- Address (all geographic subdivisions smaller than state, including street address, city, county and ZIP code)
- All elements (except years) of dates related to an individual (including birthdate, admission date, discharge date, date of death and exact age if over 89)
- Telephone number
- Fax number
- Email address
- Social Security number
- Medical record number
- Health plan beneficiary number
- Account number
- Certificate or license number
- Vehicle identifier and serial number, including license plate number
- Device identifier and serial number
- Web URL
- Internet protocol (IP) address
- Fingerprint or voiceprint
- Photographic image (not limited to images of the face)

See the HHS HIPAA website for more information: **https://www.hhs.gov/hipaa/**.

Sensitive personal information – Sensitive information is generally used to refer to confidential information whose access is subject to restrictions. It may refer to information about an individual and/or pertain to a business. There are situations in which the release of personal information could have a negative effect on its owner.

Unambiguous consent – Unambiguous consent refers to an agreement by a person to allow personal data to be collected. There are different ways that a healthcare provider may obtain such consent from a patient: opt-in consent, which means the patient explicitly agrees to permit the collection of personal data, and opt-out consent, which means that the healthcare provider assumes consent is granted until the patient explicitly revokes consent.

Government, Research and Security Information-Sharing Terms

Security information for medical devices may be sourced from many different government agencies or private organizations. Their missions range from communication or research to advisory or regulation. When referencing these organizations, it is important to define their roles and authority.

Cybersecurity and Infrastructure Security Agency (CISA) – CISA is part of the U.S. Department of Homeland Security, where it coordinates the nation's preparedness for and response to cyberthreats and incidents that affect national critical infrastructure. Examples of national critical infrastructure are healthcare, energy, transportation, financial services and communications, to name a few.

National Institute of Standards and Technology (NIST) – NIST is part of the U.S. Department of Commerce. Its activities are organized into several areas, including one for developing and publishing national cybersecurity standards.

United States Computer Emergency Readiness Team (US-CERT) – US-CERT is an organization within the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA). US-CERT is responsible for analyzing and reducing cyberthreats and vulnerabilities, communicating cyberthreat warning information, and coordinating incident response activities.

Terms to Avoid

When communicating to users and patients of connected healthcare technology, it is imperative to craft clear communications that are understandable to an audience with little or no knowledge of information technology or security. It is appropriate to use technical terms when communicating to security and IT professionals, whose responsibilities include identifying security threats and implementing recommended countermeasures. You should always consider that specific terms may not be relevant to the layperson, even if that person needs to perform specific actions to reduce security risks from successful exploitation. For this reason, the terms below should generally not be used in vulnerability communications to patients and other laypeople. Instead, we recommend using alternate terms with explanations provided in this document.

General principles for determining whether to use a more technical or security-focused term in a patient communication include the following:

- Avoid using any term that relates to a specific hardware component not commonly well known by nontechnical laypeople.
- If the term references functions and/or processes specific to the product's organization, do not reference it in a patient communication, unless the patient would need to interact with that function/process to address the security issue.
- Vulnerability communication authors should consider these questions when determining if a term should be included, substituted or provided with an explanation for a general audience:
  - Is the term known by nonsecurity professionals (e.g., encryption key, public key, protocol, least privilege)?
  - Is the term critical to communicating the intent of the message?
  - Will the intended audience understand how the term is used to support recommended actions for remediating the security incident?

continued →

Terms to Avoid (cont.)

- Per consensus of the authors of this document, the following terms should be avoided since they are overly technical:
  - Abbreviations (CVS, CVSS), including acronyms (HIPAA)
  - Coordinated vulnerability disclosure
  - Encryption key
  - Exposure
  - Least privilege
  - Nonrepudiation
  - Open-source vs. closed-source
  - Pharming
  - Protocol
  - Rectification
  - Resilience
  - Retargeting (as one type of vulnerability or threat)
  - Risk
  - Risk assessment factor
  - Verification
  - Virtual private network
  - Voiceover internet protocol (VoIP)
  - Web beacon
  - WebTrust
  - Whaling
  - Wide area network

Appendix: Vulnerability Communication Sample Template

Word version is available at **https://healthsectorcouncil.org/**.

(Company Letterhead/Logo)

- **Company name/logo**
- **What product is impacted? (Include model numbers, identifiers, software versions and other information.)**
- **What therapy does this product deliver?**

Vulnerability Summary

- Date, version (original or revision number)
- [COMPANY NAME] has learned of and evaluated a security vulnerability involving [PRODUCT].
- This vulnerability affects [PRODUCT], specifically the [PRODUCT] using software versions XXX.
- These devices are typically found in [INSERT HERE, e.g., hospital operating rooms near a patient's bedside or in chemotherapy treatment areas]. [INSERT PRODUCT CAPACITY, e.g., administer medication necessary during surgical procedures or chemotherapy treatment for cancer patients.]

Vulnerability Risk

- **Is this an update to a previous bulletin?**
- **How does this impact the delivery of care?**
- **What vulnerability and risk are associated with it?**
  - [PRODUCT NAME], with impacted software versions XXX, is vulnerable to [INSERT TECHNICAL IMPACT, e.g., unauthorized setting changes on the device]. [INSERT PATIENT IMPACT, IF APPLICABLE, e.g., These unauthorized setting changes may change or interrupt medication necessary for a patient.]
  - [INSERT STEPS CUSTOMER CAN TAKE TO CHECK FOR IMPACTED SOFTWARE VERSIONS.]
  - [INSERT INFORMATION REGARDING OBSERVED CYBERATTACK, DATA BREACH OR PATIENT HARM INVOLVING PRODUCT ASSOCIATED WITH VULNERABILITY, IF APPLICABLE.]

Response, Compensating Controls and Recommended Actions

- **What is the company doing to respond to or address the matter?**
  - Our technical teams have assessed the situation to understand any potential impact to [COMPANY NAME'S] products.
  - To date, our analysis has confirmed a [INSERT RISK TO PATIENT, e.g., high patient risk with this vulnerability].
  - [INSERT REMEDIATION TAKEN, e.g., COMPANY NAME has developed a patch that fully mitigates this risk.]
  - [INSERT HOW CUSTOMER WILL RECEIVE REMEDIATION, e.g., Field representatives will install the update at their next scheduled visit.]

- **What can the reader do?**
  - Additionally, [COMPANY NAME] recommends that [INSERT ADDITIONAL ACTIONS CUSTOMERS CAN TAKE, e.g., customers can disconnect INSERT PRODUCT NAME from the hospital network; doing so completely mitigates the vulnerability until the software update can be made by the INSERT COMPANY NAME representative].

For More Information

- **Contact information**
- **Additional background (details on researcher, if needed)**
- **General statements on company's commitment to security**
  - For more information, technical details or other questions, email [INSERT EMAIL HERE] or call [INSERT PHONE NUMBER HERE].

Additional Background

- [INSERT RESEARCHER NAME] from [VENDOR COMPANY] discovered this vulnerability and engaged [INSERT COMPANY NAME], via our established Coordinated Vulnerability Disclosure process.
- At [COMPANY NAME], we take cybersecurity seriously and have teams actively engaged in these matters. We monitor our products and systems to assess any impacts associated with cybersecurity issues and take appropriate action, as needed.
- Additionally, [COMPANY NAME] will continue to follow established coordinated disclosure processes for any significant security vulnerabilities associated with our products or any updates associated with these vulnerabilities.