Health Sector Coordinating Council
Cybersecurity Working Group

Manage Risks

Secure Medtech

Medtech Vulnerability Communications Toolkit

OCTOBER 2023

Reprint of 2022 Edition

Table of Contents

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 support delivery of healthcare services. In addition, millions of patients utilize implanted or wearable devices to support monitoring healthcare vitals or even delivering therapy. Whether in a hospital or used 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 of medical devices 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 the devices are in use. In healthcare technology, these vulnerabilities can lead to breach of sensitive information and the potential to cause patient harm. Transparency and effective communication of vulnerabilities to the individuals who use medical devices is 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 risk. Healthcare stakeholders often don't possess the experience and knowledge to translate technical information to effectively inform patients of potential risks and necessary actions. In October 2021 the FDA published "Best Practices for Communicating Cybersecurity Vulnerabilities to Patients"[1] that provided essential guidance to improve communication of cybersecurity vulnerabilities to patients.

The Health Sector Coordinating Council (HSCC) Cybersecurity Working Group (CWG) built upon 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 toolkits to support effective vulnerability communications processes and improve the clarity of messaging to non-technical 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 written to provide specific guidance to medical device manufacturers and software developers for creating cybersecurity vulnerability communications related to their products or services. The guidance focuses on vulnerability communications directed to non-security professionals, including clinicians, patients, users, or other readers not familiar with cybersecurity and connected technologies. This toolkit is intended to help medical device

1 FDA's Best Practices for Communicating Cybersecurity Vulnerabilities to Patients: https://www.fda.gov/media/152608/download

manufacturers formulate and communicate vulnerability disclosures that all affected audiences, including non-technical stakeholders, can understand.

Future versions will focus on more technically-oriented audiences in biomedical engineering and cyber security roles.

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 in 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 the largest HSCC working group of more than 400 healthcare providers, pharmaceutical and medtech companies, payers and health IT entities partnering with government to identify and mitigate cyber threats to health data and research, systems, manufacturing and patient care. The CWG membership collaboratively develops and publishes freely-available healthcare cybersecurity best practices and policy recommendations, and produces outreach and communications programs emphasizing the imperative that cyber safety is patient safety.

Acknowledgements

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 Communication Toolkit and Glossary. Some individuals listed have changed affiliations since the first publication.

Abhishek Agarwal

Task Group Co-Chair
Chief Information Security Officer
Fresenius Medical Care

Chris Tyberg

Task Group Co-Chair
Division Vice President, Product Security
Abbott

Jessica Wilkerson, J.D.

Task Group Co-Chair
Senior Cyber Policy Advisor, Center for Devices and Radiological Health
FDA

Matt Russo

Vulnerability Toolkit Task Group Workstream Lead
Sr. Director Product Security
Medtronic

Laura Robb Élan

Glossary Task Group Workstream Lead
Associate Director - Digital Health, Software, and Cybersecurity
Baxter Healthcare

Ashley Bellus

Sr. Manager of Product Security
Smith+Nephew

Uma Chandrashekhar
Global Product Security Information Officer
Alcon

Iain Deason
IT Security Specialist
CISA

Chris Reed
Director of Regulatory Policy
Medtronic

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 Analysts, Product Security
Abbott

Judd Larson
Principal Product Security Technologist
Medtronic

Nastassia Tamari
Director, Information Security Operations
BD (Becton Dickinson & Company)

Varun Verma
Regulatory Standards Specialist
Royal Philips

Erika Winkels
Director, Corporate Communications
Medtronic

Jennifer Wolf
Associate Director, Cybersecurity Communication
BD (Becton Dickinson & Company)

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:

- 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 requiring information are adequately considered.
- Vulnerability Communication 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 excessive background or experience in healthcare security.

    - Terms that should NOT be used are also included to help guide communications to be accessible for laypeople, those without professional or specialized knowledge in security.
- Vulnerability Communication Sample Mockup:
    - A sample mockup for developing a vulnerability communication.

Vulnerability Communications Overview

Communicating cybersecurity vulnerability information is complex and even more difficult when communicating to stakeholders who may not be familiar with technical terminology or understand the balance between cybersecurity risk 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 in developing a medical device vulnerability communication and how to leverage other resources in this document.

Step 1.	Categorize the vulnerability to ensure proper prioritization and consideration for target stakeholders that will need to understand and take action based on the vulnerability communication. Leverage the **Vulnerability Communication Prioritization Table** to collect necessary information that will be needed to support an effective vulnerability communication.
Step 2.	Draft vulnerability communications based on the information captured in the Vulnerability Communication Prioritization Table. The **Sample Mockup Communication** included as an Appendix can be leveraged if your organization does not already 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 for a general audience, not a security expert. Consider the specific stakeholder that must take action or would require the information as identified in the vulnerability categorization. • Leverage the **Glossary of Terms** in this document for support, both for terms to leverage 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 refine and to refine and ensure language and format are appropriate for your organization.

Vulnerability Categorization

The following graphic can be used to help categorize a vulnerability to assist in prioritizing stakeholder communication. Prioritization in the context of the table below is not focused on communication order but on identifying primary audience(s) to assist in ensuring that the communication best meets the needs of the audience for which it is intended and most needed to ensure vulnerability response.

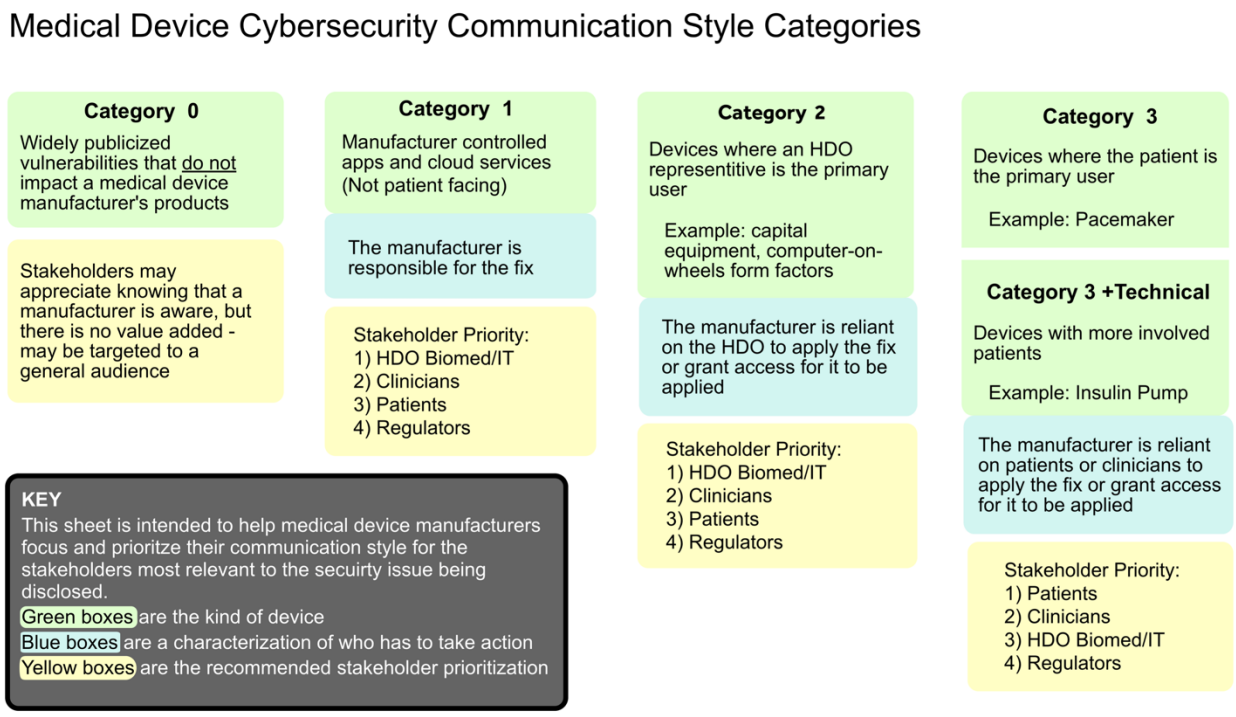

Figure 1: Categorization of Vulnerabilities

Vulnerability Communication Prioritization Table

Provides guidance for what information to collect, include and prioritize in a vulnerability communication, with important content appearing earlier in the disclosure. The content in this guide is prioritized in the order by which it appears in the table with the most important content towards 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 initial date of publication and complete history of revisions.	
What device is impacted?	Include information to identify impacted device as appropriate (may include entire device line / family, if applicable): • Images of the device; • brief device description; • model name; • model number(s); • version; • Unique Device Identifier (UDI); • Software versions affected; • and 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/understandability of the vulnerability.*	
How does this impact care delivery?	A cybersecurity bulletin is 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?	Explanation for cybersecurity vulnerability communication should include focused risk for: • Patients • Doctors • Health Delivery Organization (HDO) or Biomedical Engineering • Other relevant stakeholder If appropriate, content may be duplicative to best communicate to different audiences. Choice of which audiences to address directly is dependent on the type of device, its intended use, and the type of vulnerability.	

	Refer to the 'Communication Categories' document included as part of this kit for further guidance.	
What actions are you taking to address the risk?	Actions should include activities the medical device manufacture has complete control over.	
What actions can a user of the device perform?	Compensating controls or recommendations should be included. This includes industry best practices for cybersecurity such as network segmentation, physical controls, etc.	
Contact Information	Contact information should include support departments for both technical customer support and a non-technical contact, if feasible. Ensure that contact information is Global and not market / region specific.	
What other relevant information should be included? (Not all information is required. MDM should provide as much information as possible to provide clarity on the fix or mitigation)	Other relevant information to consider includes: • Security researcher or vendor who reported 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, but to provide explanations for common security terms that may be used in vulnerability communication so that they are accessible and understandable by 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 high school with no specialty training in technology. In addition to explaining common terms, this document makes recommendations about terms to avoid when crafting communications for the reader 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

Security Terms

Security terms are general terms that apply across all devices and software development organizations and provide a roadmap 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 describe specific goals, risks, and methods related to security.

Advisory - A communication that provides information about a security issue related to a specific product or service. Information should include 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, a text message, a website, or a physical document that is sent to specific users of a product or service. Also known as a bulletin or vulnerability note.

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

Authentication - Authentication is the process of recognizing and affirming a user's identity. Authentication will typically use specific information about a user such as something they know (a password, security question), something they are (a fingerprint, facial recognition), or something they have (an email address, mobile phone number). Multi-factor authentication will include more than one type of information to assure a person's identity. For example, a banking website will ask a user to enter their username and password (something they know), and then will 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 a specific product, file, data, or information. For example, when a user enters their username and password, the security system can then determine what types of activities or information they can access. In most cases, their authorization is limited to only those functions or data that is needed to perform the types of interactions they need.

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

Confidentiality / Confidential - In computer security, the term confidential 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 entity. Confidential information could include an individual's personal information identity such as a name, age, address, or insurance information, as well as information about their health and healthcare such as health conditions or medications.

Controlled Risk - Controlled risk is a term that the U.S. FDA has defined in its cybersecurity guidance "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 the controls versus risk is determined by the product's manufacturer.

Cybersecurity - 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 organization. Cybersecurity is often called information security or simply, security.

Encryption - Encryption is the process of modifying data or information so that is it not recognizable or readable by a human. Encryption is performed using pre-defined calculations called "algorithms" that have a "key". In order 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 the data.

Exploitability - Exploitability describes how easily a security vulnerability can be used in order to achieve the desired outcome such as stealing information, destroying computer systems or their ability to perform their intended functions. Not all security vulnerabilities are easy to exploit, therefore product manufacturers, systems owners, and/or security researchers will often evaluate how easy it is to compromise a system using an identified exploit and then plan an appropriate response, such as countermeasure or vulnerability communications. See also Exploit in SECURITY THREATS

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

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

Retention - The amount of time that information is stored in a computer system.

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

Security Researcher - A security researcher is someone who uses deep-technical knowledge in 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 that contained sensitive data that should not have been available to the public. Some security researchers may work in an academic environment in which they are identifying these weaknesses for the purposes of sharing the information with a broad audience. Other security researchers may be

interested in identifying weaknesses so that they can collaboratively share the information with the entities which can fix the weakness. 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 harming them. Some security researchers may identify these weaknesses for the purposes of either exploiting the weakness for their own malicious intent, or to share those weaknesses with others who will maliciously exploit the weakness. These researchers are sometimes referred to as black hat hackers.

Uncontrolled Risk - Uncontrolled risk is a term that the U.S. FDA has defined in its cybersecurity guidance 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 the controls versus risk is determined by the product's manufacturer.

Security Threats

A security threat is any number of things that can damage computer systems or data that resides within computer and network systems. There are different kinds of threats, but the most common types of security threats are actions that are performed by cybersecurity criminals. Some threats include breaking into computer systems or networks by guessing or "cracking" the system security such as passwords. Another type of threat can include malicious software, or "malware", that can be loaded onto computer systems or networks – often via email with malicious links - and perform many different types of damaging effects. Security threats can even include natural disasters such as hurricanes, tornados, earthquakes, or fires that may destroy buildings or equipment that support 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 way that is not specified can be considered a security threat. This section of the glossary will describe several of the more common security threats.

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

Denial-of-service (DoS) - A type of cyber-attack 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 technique is sending invalid network requests to consume available network resources of an online service.

Exploit - A program or methodology created that takes advantage of a vulnerability in a system or product to gain unauthorized access or negatively affect proper operation.

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

Malware - Malware is a term that is short for "malicious software". Malicious software can be a computer virus or other type of software code that is used to steal information, destroy data, or make systems unusable. Malware is a tool cyber criminals will often use to achieve those goals.

Phishing - Phishing describes a technique used to trick people into providing sensitive information like credit card or login information. It is also an approach to trick people into taking an action like viewing a web page or opening an attachment that will install malware on their computer or mobile device.

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

Worm - A computer worm is a type of malicious software, also called malware, that starts by infecting a computer or a computer network. Once it is able to save itself in the computer system memory or within the network hardware, it begins to make copies of its software program. These copies are moved to other parts of the computer system or network, causing a very large malware infection. Sometimes "worms" will have software that does damage to the system, but often worms do not attack the systems directly. They continue to make copies of themselves and through this action alone they can cause damage to computer systems by using up all the memory or network resources that can result in "crashing" a computer system.

Healthcare Terms

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

Electronic Health Record (EHR) - A digital record of health care 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. Also known as Electronic Medical Records (EMR).

Healthcare Provider - A person or organization that furnishes health care services and supplies, or that bills or is paid for them. Health care providers can be individuals (doctors, nurses, pharmacists, lab technicians) or organizations (hospitals, clinics, practice groups—along with their administrative staff). Health care 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 will often be necessary to include terms that describe information technology equipment, software components, or specific methods when describing how vulnerabilities have affected security and privacy. Often, technology terms may be unfamiliar to users of the systems who do not have knowledge in computing hardware, software, or security methods. This section will provide explanations of common technical terms that are frequently found in

vulnerability communications. It is not our goal to define or redefine these terms but to provide information that explains the term and provides real-world examples to better clarify the use of these terms in vulnerability communications.

Application - Software or technology tool that is designed to help someone perform a specific activity. Examples of applications include fitness trackers, word processing programs, photo editing programs, or mobile phone navigation programs.

Cloud Computing - In a computer system, cloud computing is the practice of using a network of remote servers connected using the internet to store, manage, and process data, rather than a local computer server or a 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 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, https://healthsectorcouncil.org, or http://yale.edu.

Privacy and Personal Information Terms

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

Personally Identifiable Information (PII) - PII, is a general term that is used to describe any form of sensitive data that could be used to identify or contact an individual and is a superset of PHI. PII includes: social security numbers, phone numbers, mailing or email addresses, login IDs, digital images, IP addresses, social media posts or other digital forms of data.

Privacy Policy - A policy that defines and governs how an entity, such as a hospital or doctor's office, will handle the personal information of their employees and clients. The policy will often include 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 will also define the specific rights that each data owner has that define how their data may be used or to whom it may be communicated.

Protected Health Information (PHI) - Protected health information is often shortened to PHI, or in the case of electronic health information, ePHI. Under the US HIPAA Privacy Rule, PHI is individually identifiable health information held by a covered entity, such as a healthcare provider or health plan, or their business associates. PHI includes these 18 identifiers as well as any other characteristic that could uniquely identify the 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 numbers
- Fax number
- Email address
- Social Security Number
- Medical record number
- Health plan beneficiary number
- Account number
- Certificate or license number
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web URL
- Internet Protocol (IP) Address
- Finger or voice print
- Photographic image - Photographic images are not limited to images of the face.

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

ePHI – Electronic Protected Health Information – PHI that is maintained or transmitted in an electronic format, such as in an Electronic Health Record (EHR) or Electronic Medical Record (EMR).

Sensitive Personal Information - Sensitive information is used in a general sense to mean confidential information whose access is subject to restriction and may refer to information about an individual as well as that which pertains to a business. There are situations in which the release of personal information could have a negative effect on its owner.

Unambiguous Consent - An agreement by a person to have personal data collected. There are different ways that a healthcare provider may obtain consent from a patient. "Opt-in" consent means that the patient explicitly agreed to permit the collection of their data. "Opt-out" consent means that the healthcare provider assumes consent is granted until the patient explicitly revokes their consent.

Government, Research, and Security Information Sharing Terms

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

Cybersecurity and Infrastructure Security Agency (CISA) - Cybersecurity and Infrastructure Security Agency (CISA), a part of the U.S. Department of Homeland Security. CISA coordinates the nation's preparedness for and response to cyber threats and incidents affecting national critical infrastructure. Examples of national critical infrastructure include Healthcare, Energy, Transportation, Financial Services and Communications to name a few.

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

United States Computer Emergency Readiness Team (US-CERT) - The United States Computer Emergency Readiness Team (US-CERT) is an organization within the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA). US-CERT is responsible for analyzing and reducing cyber threats, vulnerabilities, communicating cyber threat 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 communication that is clear and understandable to an audience that may have no or little understanding 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. However, one should consider how specific terms may not be relevant to the layperson, even if that person will need to perform specific actions to reduce security risks from successful exploitation. For this reason, we recommend that the following terms not be used in vulnerability communications to patients and other laypeople. We recommend alternate terms with explanations provided in this document.

General principles when determining whether to use a more technical or security focused term in a patient communication include:

- If the term relates to a specific hardware component that is not generally well-known by non-technical laypeople
- If the term references functions and/or processes that are specific to the product organization, do not reference in a patient communication unless the patient would need to interact with that function or process to address the security issue
- Vulnerability communication authors should consider the following questions when determining if a term should be included, substituted, or provided with an explanation for a general audience:
- Is the term known by non-security professionals? Example: 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 the recommended actions to remediate the security incident?
- Per consensus with the team authoring this document, the following terms were considered but would be terms to avoid given they are overly technical:
    - Acronyms in general (CVS, CVSS)
    - coordinated vulnerability disclosure
    - encryption key
    - exposure
    - Least Privilege

- Non-repudiation
- Open-source vs. closed-source
- Pharming
- protocol
- Rectification
- Resilience
- Retargeting (as one type of vulnerability or threat)
- Risk
- Risk Assessment Factors
- Verification
- Virtual Private Network
- Voice Over Internet Protocol
- Web Beacon
- WebTrust
- Whaling
- Wide Area Network

Appendix: Sample Mockup of a Vulnerability Communication

[COMPANY LETTERHEAD/LOGO]

- *Company name/logo*
- *What product is impacted? Include model numbers, identifiers, software versions, or any 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 care delivery?*
- *What is the vulnerability and the risk associated with it?*

[PRODUCT NAME] with impacted software versions XXX are 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/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 which 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 disconnect INSERT PRODUCT NAME from the hospital network*, doing so completely mitigates the vulnerability until the software update can be made by the [COMPANY NAME] representative.]

For More Information

- *Contact information*
- *Additional background – detail on the researcher if needed*
- *General statements on company's commitment to security*

For more information technical detail 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 impact associated with cybersecurity issues and take appropriate actions 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