EXECUTIVE SUMMARY FOR THE PATIENT ENGAGEMENT ADVISORY COMMITTEE MEETING

Cybersecurity in Medical Devices: Communicating Safety Concerns and Empowering Patients

SEPTEMBER 10, 2019

TABLE OF CONTENTS

Disclaimer: This Executive Summary is for discussion purposes only and does not represent draft or final guidance. It is not intended to propose or implement policy changes regarding communication of cybersecurity safety concerns.

OVERVIEW

Historically, medical devices—such as surgical laser systems, pacemakers, blood pressure cuffs, dialysis systems, MRI machines, artificial hips, laboratory diagnostic tests—were standalone technologies implanted in patients or used in hospitals or clinics to diagnose, treat, or manage health conditions. Today, the number of medical devices with a software component has flourished, and these technologies are increasingly interconnected through networked systems including wireless technologies. In hospitals, for example, many life-sustaining and supporting devices are interconnected, including cardiac monitors, insulin pumps, glucose monitors, and implantable neurostimulators.

The ability to interconnect medical devices and systems can improve patient monitoring and clinical outcomes,[1] increase efficiency of delivering medical care, improve the user experience with the medical device, and allow for more frequent device software updates. However, these capabilities and interconnectedness expose the potential for safety and integrity errors, privacy violations, and compromised medical device availability.[2]

Cybersecurity risks have become a growing concern for the medical device industry. With the increased integration of Internet and network-connectivity in health care, cybersecurity incidents have rendered medical devices and hospital networks inoperable, disrupting the delivery of patient care across health care facilities in the United States and globally.[3] Medical device safety and security is the responsibility of the entire medical device community, which includes device manufacturers, regulators, health care institutions, health care providers, and patients. While manufacturers are responsible for designing a reasonably secure device and providing updates to the device as needed to maintain adequate security, every stakeholder involved contributes to identifying issues and ensuring devices have the most up-to-date and secure software available.

[1] Heart Rhythm Society. *HRS Expert Consensus Statement on remote interrogation and monitoring for cardiovascular implantable electronic devices*. https://www.heartrhythmjournal.com/article/S1547-5271(15)00565-2/pdf (accessed June 16, 2019).

[2] IEEE Pervasive Computing. *Security and privacy for implantable medical devices*. Available at https://spqr.eecs.umich.edu/papers/b1kohFINAL2.pdf (accessed June 16, 2019).

[3] Symantec. *What you need to know about the WannaCry Ransomware*. Available at https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack (accessed on June 16, 2019).

Effective communication is integral to empowering all entities within the medical device community to safely and effectively use the devices and keep the device secure; however, communication about cybersecurity risks can be challenging. Not only is the timing of the communication important, but also what message is being communicated, how to frame the safety risks when there are no probabilities that appropriately describe it, and how to reach all the patients and providers impacted by the device. In response to these challenges, the FDA is engaging with patients, health care providers, manufacturers, and others in the medical device community to further understand effective approaches to communicate such risks and the potential role patients and health care providers can play in ensuring their medical devices are safe and effective.

MEDICAL DEVICE CYBERSECURITY BASICS

Cybersecurity is the process of preventing unauthorized access, modification, misuse or denial of use, or the unauthorized use of information that is stored, accessed, or transferred from a medical device to an external recipient.[4] It is a widespread issue affecting software-enabled medical devices connected to the Internet, networks, and other devices.

Key concepts associated with cybersecurity include:

- **Asset:** The people, property, and information to be protected. In medical device cybersecurity, assets include the patient, the medical device, and data transmitted about the patient.
- **Threat:** Anyone or anything that can exploit a vulnerability, intentionally or accidentally, and steal, damage, or destroy an asset. In medical device cybersecurity, the threat is often an unauthorized person who intentionally accesses and controls a device and uses that access to issue commands to the device.
- **Vulnerability:** A weakness or gap in a security program or protocol that can be exploited by threats to gain unauthorized access to an asset. In medical device cybersecurity, the vulnerability is typically associated with a security gap in the software or firmware used by the device.
- **Risk:** The ***potential*** for loss, damage, or destruction of an asset which occurs when a threat exploits a vulnerability. Risk is the intersection of assets, threats, and vulnerabilities. In medical device cybersecurity, the risk is typically associated with an unauthorized person (threat) accessing the device(s) of one or more patients by exploiting a vulnerability (such as a security weakness in the device's software or

[4] FDA. *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices*. Available at https://www.fda.gov/regulatory-information/search-fda-guidance-documents/content-premarket-submissions-management-cybersecurity-medical-devices-0 (accessed June 24, 2019).

firmware). Examples include inappropriate pacing or shocks from a pacemaker or inappropriate dosing from an infusion pump.

THE IMPORTANCE OF UPDATES TO MITIGATE CYBERSECURITY RISKS

While rare, the potential exists for unauthorized outside parties to exploit medical device vulnerabilities and compromise device function, potentially leading to patient harm. In addition, there are risks of compromised privacy (unauthorized access to patient or device information) or data integrity. This underscores the importance of ensuring medical devices are promptly patched and updated once vulnerabilities or risks are identified.

In general, designing and building medical devices to be completely free of errors and vulnerabilities is challenging. It is not always possible to anticipate all kinds of threats which may emerge once a medical device is in use. Software updates and patches are a necessary part of reducing medical device cybersecurity risk and maintaining patient safety.

Because of the complexity and potential impact of device vulnerabilities that are left unaddressed, the FDA works with key stakeholders throughout the community to learn more about the real-world use of medical devices from the perspective of the patient and the health care provider as well as the strategies and protocols manufacturers and health care delivery organizations employ to secure their devices.

THE FDA'S WORK IN CYBERSECURITY

The FDA has taken an agile approach to medical device cybersecurity to reflect its rapidly evolving nature, issuing final guidance documents on premarket[5] and postmarket[6] medical device cybersecurity in 2014 and 2016 respectively, and most recently, releasing an updated premarket draft guidance in 2018.[7] The draft guidance on premarket medical device

[5] FDA. *Content of premarket submissions for management of cybersecurity in medical devices—Final guidance for industry and FDA.* Available at https://www.fda.gov/regulatory-information/search-fda-guidance-documents/content-premarket-submissions-management-cybersecurity-medical-devices-0 (accessed June 24, 2019).

[6] FDA. *Postmarket Management of Cybersecurity in Medical Devices*. Available at https://www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices (accessed June 24, 2019).

[7] FDA. *Content of premarket submissions for management of cybersecurity in medical devices—Draft guidance for industry and FDA.* Available at https://www.fda.gov/regulatory-information/search-fda-guidance-documents/content-premarket-submissions-management-cybersecurity-medical-devices (accessed June 24, 2019).

cybersecurity[8], once finalized, will provide updated recommendations to medical device manufacturers regarding cybersecurity device design, labeling and the documentation that should accompany devices with cybersecurity risk. The final guidance on postmarket medical device cybersecurity provides recommendations on the postmarket maintenance, surveillance, and response to identified cybersecurity vulnerabilities and exploits of marketed products. Some of the key principles of these guidance documents are listed below.

PREMARKET CYBERSECURITY GUIDANCE

- Medical device cybersecurity is a shared responsibility among stakeholders, including health care facilities and providers, patients, and manufacturers of medical devices;
- It is important to address cybersecurity during the design and development of the medical device; and
- Establishing design inputs for device-related cybersecurity and a cybersecurity vulnerability and management approach is necessary as part of the software validation and risk analysis.[9]

POSTMARKET CYBERSECURITY GUIDANCE

- Use a risk-based framework to assure risks to public health are addressed in a continual and timely fashion;
- Articulates manufacturer responsibilities for cybersecurity of medical devices by leveraging existing Quality System Regulation and postmarket authorities;
- Foster a collaborative and coordinated approach to information sharing and risk assessment; and
- Align with Presidential Executive Orders and National Institute of Standards and Technology (NIST) Framework.

Both final guidance documents emphasize the importance of the total product lifecycle approach to medical device cybersecurity in minimizing risk (for example, through vulnerability analyses, risk assessments and threat modeling), promoting timely response and mitigation strategies, and reducing the potential for patient harm. The recommendations in the premarket

[8] FDA. *Content of premarket submissions for management of cybersecurity in medical devices—Draft guidance for industry and FDA.* Available at

https://www.fda.gov/regulatory-information/search-fda-guidance-documents/content-premarket-submissions-management-cybersecurity-medical-devices (accessed June 24, 2019).

[9] 21 CFR 820.30(g).

and postmarket final guidance documents can help assure that marketed medical devices are sufficiently resilient and responsive to cybersecurity threats.

COLLABORATION & PARTNERSHIP

The FDA convenes and actively participates in public workshops and webinars on cybersecurity as well as collaborating with various parties to foster cybersecurity awareness within the cybersecurity and healthcare community, including patients and health care providers.[10] Some examples of these workshops and collaborative outreach efforts include the following:

- Hosting an internal patient cybersecurity keynote talk and patient panel on medical device cybersecurity as part of National Cybersecurity Awareness Month (October 2017);
- Participating in the Department of Commerce's National Telecommunications and Information Administration's (NTIA) multi-stakeholder engagement initiatives that have included cybersecurity vulnerability coordination, Internet of Things (IoT) security upgradability and patching, and software component transparency (2015 to present);
- Attending CyberMed Summits hosted by the University of Arizona College of Medicine in Phoenix, the Atlantic Council and I am The Cavalry for cybersecurity clinical simulations to raise awareness among the provider community, and bringing together critical stakeholders to highlight today's challenges (2017 and 2018); and
- Participating in industry, professional society and cybersecurity conferences regularly to exchange insights with health care delivery organizations (HDOs), security researchers, industry experts, academics, health care providers, patients and others across the private sector and government.

In addition, the FDA often collaborates with professional health care organizations, patients, federal agencies, and others in the cybersecurity community to create and share information about cybersecurity with the public. Some key communication and publication activities are as follows:

- Issuing Medical Device Safety Communications on eight unique cybersecurity issues;
- Publishing an FDA fact sheet that concisely dispels common myths held by medical device manufacturers and health care delivery organizations with respect to medical device cybersecurity;[11]

[10] FDA. *Cybersecurity*. https://www.fda.gov/medical-devices/digital-health/cybersecurity (accessed August 3, 2019).

[11] FDA. FDA Fact Sheet: The FDA's role in medical device cybersecurity. Available at https://www.fda.gov/media/103696/download (accessed on June 22, 2019).

- Publishing an FDA editorial in *Pacing and Clinical Electrophysiology (PACE)* entitled "An overview of the security of cardiac implantable electronic devices," (June 2017);[12]
- Co-authoring with the MITRE Corporation the medical device cybersecurity landscape paper, "AAMI BI&T: The Evolving State of Medical Device Cybersecurity" (March/April 2018), raising general awareness of medical device security;[13]
- Publishing an editorial about the Heart Rhythm Society's Cybersecurity Leadership Summit in which FDA actively participated (July 2018);[14,15,16]
- Co-authoring a perspective piece in the American Heart Association Journal *Circulation,* targeting physicians and their role in cybersecurity (Sept 2018);[17]
- Supporting the development of the MITRE Corporation's "Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook". The playbook describes the types of readiness activities that will enable health care delivery organizations (HDOs) to be better prepared for a cybersecurity incident involving their medical devices and gives product developers more opportunity to address the potential for large scale, multi-patient impacts that may raise patient safety concerns (October 2018);[18]
- Participating in the Healthcare and Public Health Sector Coordinating Council (HSCC), a public-private partnership representing the Healthcare and Public Health (HPH) Sector of critical infrastructure, in its release of the Joint Security Plan (January

[12] PACE. *An overview of the security of cardiac implantable electronic devices*. Available at https://onlinelibrary.wiley.com/doi/abs/10.1111/pace.13128 (accessed on June 20, 2019).

[13] S Schwartz, A Ross, S Carmody, et al. The evolving state of medical device cybersecurity. *Biomedical Instrumentation and Technology* 2018;52:103-11.

[14] The Leadership Summit included patients with implanted cardiac devices.

[15] WH Maisel, JE Paulsen, MB Hazelett, et al. Striking the right balance when addressing cybersecurity vulnerabilities. *Heart Rhythm* 2018;15:e69-70. Available at https://www.heartrhythmjournal.com/article/S1547-5271(18)30468-5/fulltext (accessed on August 9, 2019).

[16] DJ Slotwiner, TF Deering, K Fu, et al. Cybersecurity vulnerabilities of cardiac implantable electronic devices: Communication strategies for clinicians—Proceedings of the Heart Rhythm Society's Leadership Summit. *Heart Rhythm* 2018;15:e61-7. Available at https://www.heartrhythmjournal.com/article/S1547-5271(18)30467-3/fulltext (accessed on June 22, 2019).

[17] Circulation. *CIED Cybersecurity Risks in an increasingly connected world*. Available at https://www.ahajournals.org/doi/10.1161/CIRCULATIONAHA.118.035021 (accessed on June 22, 2019).

[18] The MITRE Corporation. Medical device cybersecurity: Regional incident preparedness and response playbook. 2018. Available at https://www.mitre.org/sites/default/files/publications/pr-18-1550-Medical-Device-Cybersecurity-Playbook.pdf (accessed on June 23, 2019)

2019),[19] by its Medical Technology and Health IT Task Group, co-chaired by FDA, industry and an HDO. This plan, known as the JSP, describes best practices for implementing medical device cybersecurity and resilience recommendations, and further demonstrates the capabilities of medical device manufacturers working together with healthcare provider organizations to articulate a common vision to further safeguard patients; and

- Participating in the Medical Device Innovation Consortium (MDIC), a non-profit, public-private partnership that brings together industry, government, professional societies and advocacy organizations to add value to the intersecting needs of the medical device industry, to promote the TPLC of a medical device and to improve patient access to innovative products. FDA worked with MDIC in development of its report on medical device cybersecurity and advancing coordinated vulnerability disclosure (released Oct 2018).[20] This paper articulates the barriers impeding adoption of coordinated vulnerability disclosure policies and processes and helps inform conversations among medical device manufacturers about the value of working with security researchers and others who identify vulnerabilities. Knowing vulnerability information is critical to addressing cybersecurity risk to medical devices in a timely and coordinated manner, as well as being able to communicate recommendations to clinicians, patients and caregivers.

FDA has worked continuously to foster more positive interactions and collaborations between the security research community and medical device manufacturers. Expanding our efforts to cultivate a productive working relationship with the security research community, FDA has participated and encouraged medical device manufacturers to participate in the DEF CON Biohacking Village—Medical Device Hacking Lab with the announcement of its *#wehearthackers* initiative (January 2019). These collaborative efforts have been fruitful with ten major device manufacturers declaring their intent to bring their devices to DEF CON's Biohacking village (August 2019). DEF CON's Biohacking Village brings security researchers and medical device manufacturers face-to-face, providing an opportunity in real-time for dialogue, relationship building, and a safe environment to do research on devices. These collaborative efforts among regulators, federal agencies, security researchers, medical device industry, heath care providers and patients help cultivate tailored, forward leaning, and nimble cybersecurity solutions that drive towards improved patient safety.

[19] Healthcare Sector Coordinating Council. *Medical Device and Health IT Joint Security Plan.* Available at plan https://healthsectorcouncil.org/wp-content/uploads/2019/02/HSCC-MEDTECH-JSP-v1.2.pdf (accessed on August 19, 2019).

[20] Medical Device Innovation Consortium. *Advancing Coordinated Vulnerability Disclosure* https://mdic.org/program/cybersecurity/

UNDERSTANDING PATIENTS’ LIVES AND PERSPECTIVES IS ESSENTIAL FOR MAINTAINING MEDICAL DEVICE CYBERSECURITY

Medical devices used by patients outside the hospital or clinic are increasingly connected to the internet where the patient lives and/or through consumer devices like smartphones, tablets, computers, and smartwatches. Many patients may be unaware of the importance of these connections in maintaining and upgrading medical device functionality and security, as well as the potential cybersecurity vulnerabilities they may pose.

Due to the complexity of communication, logistics of software updates and patches, health literacy, and understanding of medical device cybersecurity, understanding patients’ perspectives is critical to implementing an actionable communication strategy. FDA has engaged patients to better understand how they interact with the software in their medical devices.

Many patients report being able to update their devices at home using their own Bluetooth or Wi-Fi enabled configuration, allowing for convenient and automatic updates. Some patients elect to have their devices updated during their clinic or hospital visit, while other patients are required to update their devices under direct medical supervision.

For patients able to update and patch devices at home, manufacturers often communicate by sending notifications to a mobile application ("app”) installed on a smartphone. Some patients also reported receiving email communication from manufacturers or a phone call from their doctor’s office. Patients living in rural settings and/or with limited access to the internet encounter unique challenges when patching or updating their devices. Many patients from these settings do not have access to smartphones, Internet, Wi-Fi, or Bluetooth enabled devices. Due to these obstacles, patients from these communities may be delayed in updating or patching their devices. Patients in these communities may also have difficulty visiting their health care provider to patch or update their medical devices. Understanding these challenges and developing pragmatic approaches are important steps to assure that these patients’ medical devices remain cybersecure.

COMMUNICATING MEDICAL DEVICE SAFETY CONCERNS TO PATIENTS AND THE PUBLIC

When a safety concern exists for a medical device, it is critical to communicate to impacted groups. Multiple organizations often communicate about the safety concern, including the manufacturer of the impacted medical device, the FDA, the media, patient safety organizations and other entities. Because safety depends in part on the patient and/or health care provider users, FDA aims to educate the public about the appropriate use of FDA-regulated products when it communicates about safety concerns.

Generally, the FDA develops message content specific to audiences with different informational needs, such as patients[21], health care providers, hospitals, and manufacturers. This messaging is then developed into a communication product(s) (for example, a Safety Communication, Press Release, and Letter to Health Care Providers). The communication product is then distributed through various communication channels, such as posting on the FDA's website, direct email and social media.

"Plain language" refers to writing in a way that helps readers understand the content in a document the first time they read it. Communicating clearly gets the point across quickly without using unnecessary words or technical jargon and increases the chance information will be understood and used. Writing in plain language is a communication best practice. It is not unprofessional and does not "dumb down" the message or "talk down" to the audience. The Plain Writing Act of 2010 requires all federal agencies to use plain language whenever they communicate with the public. [22]

Communicating during emergency events, such as a safety concern with a medical device, presents unique challenges. Over the course of the FDA's investigation of an issue, both the FDA and industry gather more information. This can potentially result in significant changes in recommendations for patients, or health care providers, which can lead to confusion. Effective communication is needed to ensure that patients can understand the issue, make informed choices, adapt to evolving recommendations, and take appropriate actions.

CENTER FOR DEVICES AND RADIOLOGICAL HEALTH'S APPROACH

CDRH communicates to a variety of audiences, including patients, caregivers, health care providers, medical device industry, and other external stakeholders.

- When the primary audience for communications is patients and caregivers, CDRH posts information on the FDA.gov website as a **Medical Device Safety Communication.** This typically includes a summary of the safety concern, recommendations for patients and caregivers, additional recommendations for health care providers or manufacturers, and the FDA's actions to resolve the safety concern.

- When the primary audience for communications is health care providers, CDRH posts information on the FDA.gov website as a **Letter to Health Care Providers**. These letters typically provide details on the safety concern, recommendations for health care

[21] The term patient as used in this document refers inclusively to people who receive health care services.

[22] Plainlanguage.gov. *Law and requirements*. Available at https://plainlanguage.gov/law/ (accessed on June 21, 2019).

providers, and detailed information on the FDA's evaluation of the issue and actions to resolve the safety concern.

In some cases, both approaches may be used.

DISSEMINATING MESSAGES

Communication strategies incorporate dissemination of materials through multiple channels used by target audiences. The primary methods CDRH uses to disseminate information include posting safety communications on FDA.gov, email marketing and social media to share and promote the message, and targeted outreach to impacted stakeholders. *See Appendix B, Methods for Disseminating Medical Devices Safety Messages for details.*

Often the FDA's messages are amplified as they are redistributed through other channels, such as major news outlets, trade media, advocacy groups, and other government agencies. The mechanisms vary but can include a posting on their website; a televised, radio-aired or published news story; redistribution through an email to their stakeholders; or inclusion in their newsletter.

EVALUATING THE EFFECTIVENESS OF SAFETY COMMUNICATIONS

The agency uses available metrics to determine the reach of its safety communications pages on FDA.gov (how many people viewed the page, whether they read the content, which country they came from), but data on variables such as demographics are not currently available. Likewise, CDRH can measure email and social media reach (how many people opened the email or liked a tweet), but specific feedback on the page is not currently assessed. An agency-wide voice of the customer (VOC) survey is being implemented on FDA.gov, and CDRH may have opportunities to use that system to get patient feedback on its safety communications.

Techniques that have been used to evaluate the effectiveness of safety communications include:

- Surveys
- Evaluations from risk communication experts
- Message testing
- Usability testing of content and navigation
- User data on interactions with the safety communication

GENERAL CHALLENGES WITH COMMUNICATING SAFETY CONCERNS

CDRH encounters several challenges communicating on safety topics in general. These challenges include audience health literacy, the effects of stress experienced by target audiences, language barriers, and barriers to Internet use.

LIMITED HEALTH LITERACY

Health literacy is defined as the degree to which individuals have the capacity to obtain, process, and understand basic health information and services needed to make appropriate health decisions.[23] The prevalence of low health literacy and marginal health literacy is estimated to be 26% and 20%, respectively in the US, which amounts to 46% total with limited health literacy.[24] Health literacy affects people's ability to navigate the healthcare system, fill out complex forms, engage in self-care and chronic disease management, and understand mathematical concepts such as probability and risk.[25] Low health literacy has been linked to poor health outcomes and decreased utilization of preventive health services.[26] According to the Department of Health and Human Services, in addition to basic literacy skills, health literacy requires knowledge of health topics. Studies have found that people with low health literacy and illness have less knowledge of illness management and of health-promoting behaviors than those with higher health literacy.[27,28,29] Health information is equally challenging for persons with advanced literacy skills as medical science progresses rapidly and what people may have learned about health during their school years is often incomplete, outdated, or forgotten. Hence, people can be very well-educated and highly literate in their area of expertise, and still not fully understand complex medical information. Regardless of one's literacy level, when unfamiliar, technical language is used, or information concerning a safety concern is presented, it is difficult to fully comprehend the information.

IMPACT OF STRESS ON TARGET AUDIENCES

Research from the risk communication field suggests that audiences who are emotional or under stress may be less receptive to communications about risk and recommended actions. As

[23] CR Selden, M Zorn, SC Ratzan, et al. *Healthy People 2010*. NLM Pub. No. CBM 2000-1. Bethesda, MD: National Institutes of Health, U.S. Department of Health and Human Services.

[24] MK Paasche-Orlow, RM Parker, JA Gazmararian, et al. The prevalence of limited health literacy. *J Gen Intern Med* 2005;20:175-84.

[25] US Department of Health and Human Services. Quick Guide to Health Literacy. https://health.gov/communication/literacy/quickguide/factsbasic.htm (accessed August 1, 2019).

[26] TL Scott, JA Gazmararian, MV Williams, et al. Health literacy and preventive health care use among Medicare enrollees in a managed care organization. *Medical Care* 2002; 40: 395-404.

[27] SC Kalichman, E Benotsch, T Suarez, S Catz, et al. Health literacy and health-related knowledge among persons living with HIV/AIDS. *American Journal of Preventive Medicine* 2000;18: 325-31.

[28] D Schillinger, K Grumbach, J Piette, F Wang, et al. Association of health literacy with diabetes outcomes. JAMA 2002;288:475-82.

[29] Institute of Medicine. (2004). Health Literacy: A Prescription to End Confusion. *Washington, DC: National Academies Press; 2004.*

described in Risk Communication for Public Health Emergencies, “when people are upset, angry, fearful, outraged, under high stress, involved in conflict, or feel high concern, they often have difficulty processing information, which is particularly important to consider when they receive crisis risk communication.”[30] The type of stress or emotion may affect how people process a safety communication. Research has shown that stress leads to a substantial decrease in the ability to learn new information, particularly if it requires using memory-related information.[31] For example, if an individual is angry, sad, or anxious, they may have less capacity to process new information or access old information that could help with understanding the new information. A person under stress may be more attentive to a message, but the focus of their attention may be narrow, which affects their ability to scan information, assimilate large amounts of information, or make complex decisions using that information. If an audience is likely to be stressed or upset, best practices in risk communication call for the key messages to be prioritized and stated simply.

COMMUNICATING TO INDIVIDUALS WITH LIMITED ENGLISH PROFICIENCY

In addition to limited health literacy and cybersecurity understanding, CDRH also faces challenges with communicating to individuals for whom English is not their first language. The 2017 results of the American Community Survey of over 120 million households found over five million households were a limited English-speaking household. Over three million spoke Spanish as their first language, with over two million speaking other languages.[32]

Additionally, using plain English will not necessarily help individuals who do not speak English as their primary language and who have limited ability to read, write, speak, or understand English. Simply translating health information into a person’s native tongue does not guarantee that non-English speakers will be able to read or understand it. To ensure understanding, health information for people with limited English proficiency needs to be communicated plainly in their primary language, using words and examples that make the information understandable in their native language.

The FDA does not always translate the material it distributes in languages other than English. For example, the cybersecurity safety communications focused primarily on recommendations

[30] Annual Review of Public Health. *Risk Communication for Public Health Emergencies.* https://www.annualreviews.org/doi/full/10.1146/annurev.publhealth.28.021406.144123 (accessed August 1, 2019).

[31] S Vogel, LM Kluen, G Fernandez, et al. Stress affects the neural ensemble for integrating new information and prior knowledge. *Neuroimage* 2018: 173: 176-87.

[32] United States Census Bureau. *Household Language: 2017 American Community Survey 1-Year Supplemental Estimates with a Population Threshold of 20,000 or More*. Available at https://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?pid=ACS_17_SPL_K201601&prodType=table (accessed on June 25, 2019).

for the US health care community and therefore have not been translated into any other languages. However, translation is generally completed when the safety concern affects a large non-English-speaking patient community.

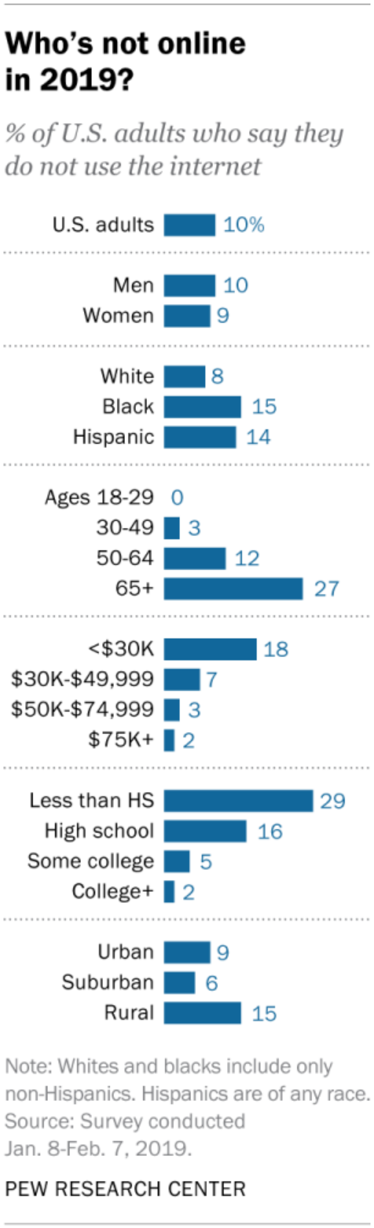
REACHING COMMUNITIES WHO MAY NOT BE ONLINE

Like other government entities, CDRH relies heavily on digital distribution mechanisms and other sources to distribute and amplify communications about safety concerns. All safety communications are posted to FDA.gov and are then distributed through email distribution lists (to which individuals have subscribed) as well as social media. These messages are amplified by other digital means, such as articles in digital media, email sharing, and social sharing. Despite the overall widespread use of digital communications, the access to or use of online resources varies considerably among different target audiences.

According to a Pew Research Center analysis of 2019 survey data,[33]10% of U.S. adults do not use the Internet.[34] The analysis found that Internet non-adoption is linked to several demographic variables, including age, household income, educational attainment, and community type.

The target audiences for safety communications who are significantly less likely to be online include:

- Older adults, particularly adults over the page of 65;
- Adults with a household income of less than $30,000;
- Adults with a lower level of education attainment, particularly adults with a high school education or less; and
- Adults who live in rural areas.



Who's not online in 2019?

% of U.S. adults who say they do not use the internet

Note: Whites and blacks include only non-Hispanics. Hispanics are of any race.
Source: Survey conducted Jan. 8-Feb. 7, 2019.

PEW RESEARCH CENTER

[33] Pew Research Center. *Fact Tank*. April 22, 2019. https://www.pewresearch.org/fact-tank/2019/04/22/some-americans-dont-use-the-internet-who-are-they/ (accessed August 1, 2019).

[34] The PEW Research Center defined adults as age 18 and older. At CDRH, the definition of adults is older than 22 years and older.

A Pew Research Center survey from 2013 [35] identified some key reasons why adults did not go online:

- 34% of Internet non-users had no interest in going online or did not think it was relevant to their lives,
- 32% considered the Internet too difficult to use, and
- 19% indicated that the cost of owning a computer or getting Internet service prevented them from going online.

COMMUNICATING MEDICAL DEVICE CYBERSECURITY CONCERNS

The FDA released Safety Communications on eight medical device cybersecurity concerns since 2013.[36] While some are stand-alone safety communications, others are related to the same device, such as the three safety communications related to Abbott's (formerly St. Jude Medical) implantable cardiac devices on January 9, 2017, August 29, 2017, and April 17, 2018. Cybersecurity issues are customarily disclosed when there is a software update to fix the issue. The three examples above represent when Abbott had fixes for issues within their implantable cardiac device system starting with the home bedside monitor, then pacemakers, and then implantable cardioverter defibrillators (ICDs).

CHALLENGES IN COMMUNICATING CYBERSECURITY SAFETY CONCERNS

For most safety messages (and specifically, those outside of the realm of cybersecurity), FDA communicates the types of harms that may result from a medical device malfunction or failure and their associated likelihood of occurring. Unlike other safety messages, cybersecurity concerns pose the unique challenge of communicating potential risks for which the probability and/or likelihood of occurrence of a successful exploit is not known. In most cases, the composite of information that would be necessary to quantify the risk in a traditional sense (which often relies on historical and/or 'evidence-based' data) is lacking, including predicting when a vulnerability may be exploited. Therefore, phrasing in terms of probabilities or likelihoods may not be the most appropriate approach to communicating information pertaining to the risk of harm with respect to medical device cybersecurity concerns.

[35] Pew Research Center. *Internet & Technology.* September 25, 2013. https://www.pewinternet.org/2013/09/25/whos-not-online-and-why/ (accessed August 1, 2019).

[36] FDA. Cybersecurity. Available at https://www.fda.gov/medical-devices/digital-health/cybersecurity (accessed on August 9, 2019).

Understanding the motivations of unidentified, unauthorized persons, predicting when they may act, identifying what vulnerabilities would be exploited, isolating the action to one type or brand of device, and capturing the risks associated with that exploit are each challenging, on their own, as independent factors; when considered in its totality, the challenge to fully quantify risk is that much more complex.

In addition, there are challenges and risks in updating devices to address cybersecurity concerns, including the potential failure to function, device damage, need for additional surgeries, and out-of-pocket costs to the patient. For example, software updates can fail at a known rate, which in the worst-case may require a surgical intervention such as exchanging the device to address the failure.

Currently, there is no suitable model or mathematical formulation that would enable risk quantification of a medical device cybersecurity vulnerability extrapolating to risk of potential patient harm. The absence of such a construct impedes informed decision making between patients and providers in determining whether the benefits of a patient receiving device updates for cybersecurity concerns outweighs the potential risks of undergoing the updates. Understanding how unknowable risks are weighed against knowable risks is critical to help address these communication challenges.

With medical device cybersecurity, the following factors are all in play and need to be given consideration: the unknowable probability of a successful exploit; the velocity with which an exploit may occur along with its distributive impact across a patient population; and the time it would otherwise take to deploy an effective countermeasure that contains and mitigates harm, (generally outpaced by the speed and scale of the exploit's impact). FDA's approach regarding medical device cybersecurity, by necessity, has been anticipatory, forward-leaning and proactive as vulnerabilities are identified and verified *before* exploit, rather than waiting for a signal or indicator of harm becoming manifest. This is an important distinction to note compared to the triggers that FDA uses to initiate other, non-cybersecurity-related safety communications.

WHEN AND HOW TO COMMUNICATE

The FDA regularly communicates to the public about known medical device safety issues, as well as emerging signals. Emerging signals are based on our initial evaluation of new information which may have the potential to impact patient management decisions and/or the known benefit-risk profile of the device. This does not include information that is unconfirmed, unreliable, or unsupported with evidence.[37]

[37] FDA. Public notification of emerging postmarket medical device signals ("emerging signals"). Available at https://www.fda.gov/regulatory-information/search-fda-guidance-documents/public-notification-emerging-postmarket-medical-device-signals-emerging-signals (accessed on August 22, 2019).

In general, communicating cybersecurity vulnerabilities and risks related to medical devices takes place when a solution is available to help mitigate the risks. The decision to communicate is to provide actionable information that mitigates risks while maintaining the benefits that medical device technologies provide.

To date, for medical device cybersecurity, the FDA has taken a proactive stance and communicated about ***potential*** concerns as opposed to waiting for harm to occur. The FDA learns about cybersecurity issues at different stages of identification:

- When first identified, this is referred to as a potential ***cybersecurity vulnerability,*** which could be identified by a researcher, news article, device manufacturer, or some other source.
- When a vulnerability is confirmed to exist by manufacturers, it is referred to as a potential ***cybersecurity risk****.*
- When there is a possibility that a human or automated actor can successfully exploit a vulnerability, it is referred to as a ***cybersecurity threat***.
- When impacts to the patient are potentially severe and there is a way to reduce risk, the FDA will communicate. Regarding timing of communication, broad discussion within the cybersecurity community-at-large yields varying views for safety-critical industries, such as the medical device sector. A prevailing perspective to which FDA adheres is that in the absence of an effective way to reduce risk, prematurely communicating can increase opportunity for exploit by highlighting a potentially unknown issue and, by extension, increasing potential exposure to harm.

A definitive fix of a vulnerability can, however, take weeks to months to develop and test before it can be deployed safely. While such a permanent solution (such as a software update) is being developed, risk reduction measures are recommended. It is important to note that such risk mitigations can potentially introduce other risks (e.g., stopping usage of a device that has many benefits to the patient), and such mitigations are often intended to only be temporary solutions (e.g., disconnecting from the internet).

CYBERSECURITY LITERACY

Cybersecurity, in general, is not well understood by audiences who are not part of the cybersecurity community. The Pew Charitable Trusts conducted a survey in 2016 to test Americans general understanding of cybersecurity.[38] The questions asked as part of the survey focused on the general understanding of cybersecurity, for example, strong passwords, use of

[38] Pew Research. *What the Public Knows About Cybersecurity*. March 22, 2017. https://www.pewinternet.org/2017/03/22/what-the-public-knows-about-cybersecurity/ (accessed August 1, 2019).

Wi-Fi, and email. The survey showed that out of 1,055 adult respondents, the typical respondent answered only five of the thirteen (38%) survey questions correctly.

The education level of the respondents impacted their ability to answer a question correctly. According to Pew's survey, individuals who had a college degree or higher answered an average of seven questions (54%) correctly. Those who have attended, but did not graduate from college, answered 5.5 questions (42%) correctly on average. Those with high school diplomas or less answered an average of 4.0 questions (31%) correctly.[39]

COORDINATION TO AMPLIFY MESSAGE DISTRIBUTION

Through formal agreements, FDA works with the following federal, public, and private sector partners:

- Department of Homeland Security (DHS)
- Health Information Sharing & Analysis Center, Inc. (H-ISAC)
- Medical Device Information Sharing and Analysis Organizations (ISAOs)

One goal of these collaborations is to create a "safe harbor" through formal mechanisms by which information regarding medical device cybersecurity vulnerabilities and threats can be shared in a trusted space. These collaborations also foster the development of a shared risk assessment framework to enable stakeholders to consistently and efficiently assess patient safety and public health risks associated with identified cybersecurity vulnerabilities and take timely and appropriate action to mitigate the risks.

Any CDRH communications related to cybersecurity are coordinated with the Department of Homeland Security's National Cybersecurity and Communication Integration Center (NCCIC) to ensure consistent messaging across agencies and ample distribution of the message. The NCCIC is a hub for information and expertise related to cybersecurity and communications information.[40] The NCCIC works to:

- Build risk awareness and help people understand how to mitigate threats and vulnerabilities;

[39] Pew Research. *What the Public Knows About Cybersecurity*. March 22, 2017. https://www.pewinternet.org/2017/03/22/what-the-public-knows-about-cybersecurity/ (accessed August 1, 2019).

[40] National Cybersecurity and Communications Integration Center. Available at https://www.dhs.gov/cisa/national-cybersecurity-communications-integration-center (accessed August 22, 2019).

- Help customers take actions to improve their risk posture and support a common operational picture of the national cybersecurity and communications risk landscape; and
- Defend federal networks and respond to significant incidents.

Depending on how the vulnerability was identified and the potential impact to patients, the FDA and the Department of Homeland Security (DHS) may also publicly communicate about device vulnerabilities and the availability of patches and updates. H-ISAC and Medical Devices ISAOs help to further disseminate the message and help provide actionable steps for stakeholders to take.

FDA communicates about medical device cybersecurity vulnerabilities only when there is a patient safety risk. From June 13, 2013 through June 27, 2019, the FDA issued 8 safety communications related to medical device cybersecurity. DHS communicates about all medical device cybersecurity vulnerabilities, regardless of whether there are patient safety impacts. DHS released 63 medical device advisories between October 23, 2013 and March 31, 2019.[41]

COMMUNICATING PREVENTION MESSAGES

In addition to communicating on cybersecurity safety concerns, CDRH routinely communicates on general cybersecurity matters. October is National Cybersecurity Awareness Month. During this month, CDRH amplifies the Department of Homeland Security's National Cybersecurity Awareness Month campaign, which provides information on cybersecurity best practices. Each week has a different theme and CDRH, in collaboration with the FDA's Office of Media Affairs, posts information on social media and sends emails through listservs to stakeholders who have subscribed to receive the information. One example of information the FDA has created includes an FDA Fact Sheet[42] on the "FDA's Role in Medical Device Cybersecurity".

CONCLUSION

[41] Medcrypt report. *Impact of monitoring on medical device vulnerabilities*. Available at https://www.medcrypt.com/medcrypt_whitepaper_4_monitoring.pdf (accessed on July 18, 2019).

[42] FDA. *The FDA's role in medical device cybersecurity*. https://www.fda.gov/media/123052/download (accessed on July 31, 2019).

Medical devices are increasingly connected, whether used in home or hospital environments. In health care facilities, network connectivity continues to expand, and business operations are increasingly reliant on digital infrastructure. While these changes provide enhanced benefits, it also creates the potential for cybersecurity risks. If not identified and adequately mitigated, such risks can potentially lead to patient harm, disruption of patient care delivery in health care facilities, privacy violations, and compromised medical device availability. With interconnected medical devices increasingly being used at home, this challenge could be amplified. For these reasons, cybersecurity is considered among the top concerns among health care leaders.[43]

Medical device safety and security is the responsibility of the entire medical device community, which includes manufacturers, regulators, health care facilities, health care providers, and patients. Designing medical devices to reduce all anticipated risks is important but cannot remove or prevent all possible risks. Many risks emerge only once medical devices are used widely in the field. For medical device cybersecurity, patches and updates are important to help mitigate risks that emerge once devices are in use. Other critical efforts to assure ongoing medical device safety is the continuous process of postmarket safety monitoring; identifying emerging safety concerns; developing ways to eliminate, reduce, or otherwise mitigate the risk; and effective communication to all parties that need to know about the safety concern and take action.

Effective communication is key to ensuring all responsible parties in the medical device community receive and comprehend the information they need to make decisions and take appropriate actions to assure continued medical device and patient safety. However, the complexity of assessing and communicating about risks which are difficult or impossible to quantify, the timing of communication about emerging cybersecurity concerns (such as before a solution is developed), and limited awareness by the US public of cybersecurity concepts makes communicating about cybersecurity risks challenging. These challenges are amplified by limited health literacy, the impact of stress on comprehension, communicating to individuals with limited English language proficiency, and reaching individuals who may not be online. With these compounded challenges resting at the intersection of medical device cybersecurity and risk communication, it is critical to understand patients' perspectives to better develop and implement, an effective and actionable communication strategy. By working collaboratively and continuing to put the patients first, the FDA can help assure the ongoing cybersecurity of medical devices that play an important role in diagnosing, treating and managing patient health.

[43] HIMSS. 2019 HIMSS U.S. Leadership and Workforce Survey. Available at: https://www.himss.org/2019-himss-leadership-and-workforce-survey-0 (accessed July 31, 2019).

APPENDIX: METHODS USED BY CDRH FOR DISSEMINATING MEDICAL DEVICE SAFETY MESSAGES

SAFETY COMMUNICATIONS ON FDA.GOV

The agency's website, FDA.gov, is the primary distribution medium for safety communication on medical devices. In 2018, medical device safety communications received 936,000 pageviews. The number of visitors viewing safety communications on mobile devices has increased steadily over the past few years, with over 60 percent of pageviews on specific safety communications coming from readers using mobile devices in recent months. Developing complex communications for the limited display space of mobile devices is a significant challenge.

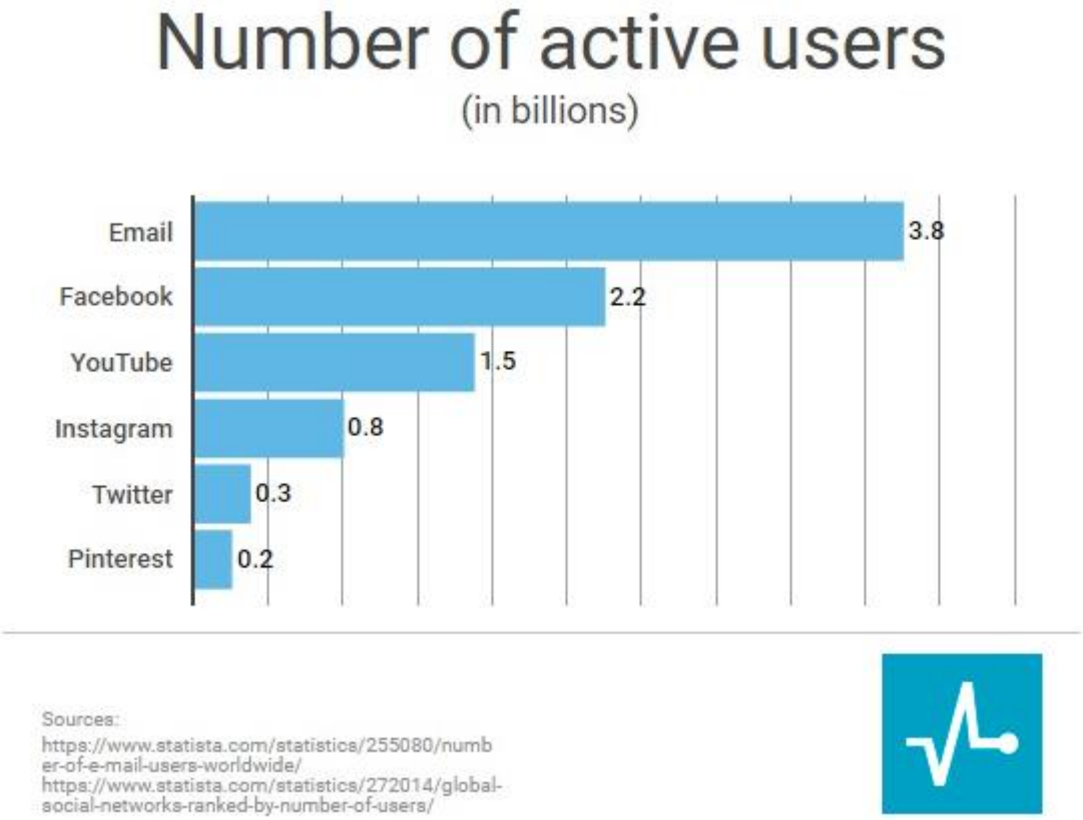
The primary source for traffic to these pages is Google and other external search engines. Readers tend to go to Google first and search rather than navigate through websites for information. Other important sources of traffic to safety communications are email marketing, social media, and referrals (links) from other websites, such as mass media sites and medical information sites. When a safety communication is first posted, most of the visitors (up to 90%) come to the page from email marketing.

EMAIL MARKETING

The email distribution lists for medical device content currently have 404,000 subscribers, with 126,000 subscribers opting to receiving safety and recall information. Safety information is also distributed through the MedWatch distribution list for safety alerts, which currently has 365,000 subscribers.

While email marketing is not a new technology for disseminating information, it remains one of the most effective with the highest return-on-investment, compared with other techniques, such as Internet ads (paid search), social media, video, and traditional media (radio and TV). While distribution to CDRH's email accounts helps to push messages out to our target audiences, it represents a fraction of the total population who may need to receive this information.

Number of Active Email and Social Media Users[44,45]



Number of active users

(in billions)

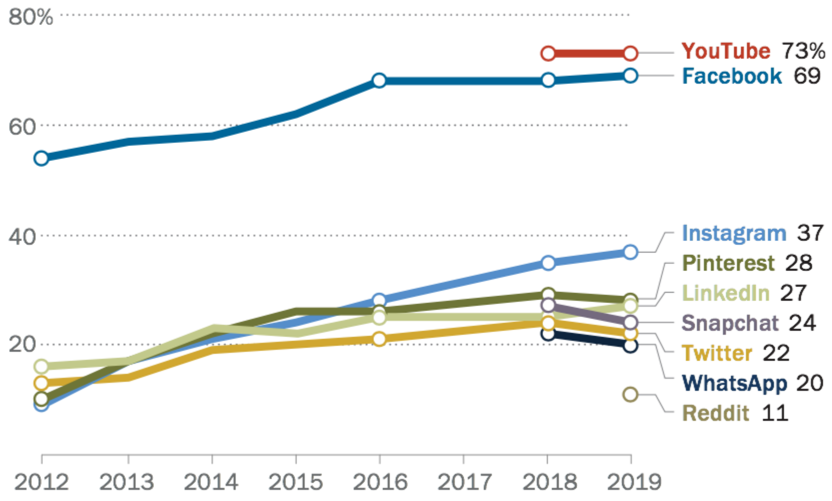
Sources:
https://www.statista.com/statistics/255080/number-of-e-mail-users-worldwide/
https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

[44] Statistica.com. *Most popular social networks worldwide as of July 2019, ranked by number of active users (in millions).* https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ (accessed on June 17, 2019).

[45] Statistica.com. *Number of email users worldwide from 2017 to 2023 (in millions).* https://www.statista.com/statistics/255080/number-of-e-mail-users-worldwide/ (accessed on July 25, 2019).

SOCIAL MEDIA

According to a Pew Charitable Trusts survey[46] conducted in early 2019, for every 10 adults, approximately seven use Facebook. That statistic remains unchanged since 2016 but represents a fifty-four percent increase in adult users since 2012. A 2018 survey from Pew Charitable Trusts[47] shows that approximately forty percent of U.S. adults get news from Facebook and approximately twelve percent of respondents in the survey receive their information from Twitter.



Facebook, YouTube continue to be the most widely used online platforms among U.S. adults

% of U.S. adults who say they ever use the following online platforms or messaging apps online or on their cellphone

Note: Pre-2018 telephone poll data is not available for YouTube, Snapchat and WhatsApp. Comparable trend data is not available for Reddit.
Source: Survey conducted Jan. 8-Feb. 7, 2019.

PEW RESEARCH CENTER

A growing amount of traffic to CDRH safety communications come from social media, primarily mobile Facebook. In most cases, approximately five percent of traffic to a safety communication comes from mobile Facebook, but the percentage can reach as high as fifteen percent.

[46] Pew Research Center. *10 facts about Americans and Facebook*. May 16, 2019. https://www.pewresearch.org/fact-tank/2019/05/16/facts-about-americans-and-facebook/ (accessed July 27, 2019).

[47] Pew Research Center. *News Use Across Social Media Platforms 2018*. September 10, 2018. https://www.journalism.org/2018/09/10/news-use-across-social-media-platforms-2018/ (accessed July 27, 2019).

Over the last several years, CDRH has increased its participation in the social media conversation through posting on Twitter, Facebook, and LinkedIn. Because of resource restrictions, the current practice in CDRH is to use social media to push out information. There have been instances where CDRH has been able to participate in some two-way conversations with consumers, such as participation in Twitter Chats, but CDRH lacks the resources to routinely engage in two-way conversations through social media.

SEARCH ENGINE PAID ADVERTISING

One effective option to reach audiences for medical device safety communications is through search engine paid advertising, such as Google AdWords. Medical device manufacturers routinely use Google AdWords to reach target audiences. Centers and offices within the FDA have conducted successful Google AdWords campaigns through the years to increase traffic to specific web pages, but limited resources prevent the FDA from using these campaigns on a regular basis.

AMPLIFYING DISTRIBUTION THROUGH PARTNERS

To help amplify and distribute safety information, CDRH works with its FDA colleagues, such as the Regional Public Affairs Specialists, Office of Media Affairs, Office of Minority Health, and Office of Women's Health to help disseminate and amplify messaging to target audiences. Each group can target specific audiences, either regionally or nationally. The collaborations with these groups allow the FDA to reach audiences outside of traditional mechanisms and provide information to audiences who may not routinely look for information from the FDA. However, there are limitations to their reach, as the Public Affairs Specialists are located in the Office of Regulatory Regional Areas, which are located mostly in urban or suburban areas. Additionally, resources are not readily available in those offices to provide information in other languages besides English.

In addition to collaborating with other parts of the FDA, CDRH also collaborates with other Federal Agencies on topics that overlap with authorities within that agency such as the Department of Defense (DOD), Centers for Disease Control and Prevention (CDC), and the Agency for Health care Research and Quality (AHRQ). These other Agencies can help the FDA disseminate information to specific audiences whom the FDA may not traditionally reach.