The ORACLE is a free newsletter *of recent medical device regulatory & computer information that may be of interest to designers, and device Manufactures.*

ORACLE

ESTABLISHED 1988
NEWSLETTER FROM **DELPHI CONSULTING GROUP** (**DCG**)
An Internet Based Medical Device Regulatory Service,
www.delphiconsulting.com

Delphi Consulting Group (DCG), *provides medical device regulatory (FDA) release to market via the 510(k) and PMA pathways. DCG is Internet based to boost efficiency and reduce costs*

Vol. 27, Issue 7 July 2021

Remanufacturing of Medical Devices; Draft Guidance for Industry and Food and Drug Administration Staff

The FDA seeks input on the draft guidance "Remanufacturing of Medical Devices." Submit comments before August 17, 2021.

Strengthening Cybersecurity Practices Associated with Servicing of Medical Devices: Challenges and Opportunities; Discussion paper

The FDA seeks input on the discussion paper "Strengthening Cybersecurity Practices Associated with Servicing of Medical Devices: Challenges and Opportunities." Submit comments before August 17, 2021.

Introduction

A remanufacturer is defined as any person who processes, conditions, renovates, repackages, restores, or does any other act to a finished device that significantly changes the finished device's performance or safety specifications, or intended use. [21 CFR 820.3(w)]. The FDA considers remanufacturing to be a distinct activity from servicing that raises different concerns, and is thus regulated differently.

The availability of timely, cost-effective, quality maintenance and repair of medical devices is critical both to the successful functioning of the United States (U.S.) healthcare system and to the continued quality, safety, and effectiveness of marketed medical devices in the U.S. This is very important for those devices used on numerous patients over long periods of time. Poor quality servicing may lead to poor device performance, device malfunction, and adverse events. Cybersecurity is also an important consideration in the servicing of medical devices.

Resources on Remanufacturing and Servicing

The distinction between "remanufacturing" and "servicing" is important to understand. Remanufacturing is the processing, conditioning, renovating, repackaging, restoring, or any other act done to a finished device that significantly changes the finished device's performance or safety specifications, or intended use. Servicing is the repair and/or preventive or routine maintenance of one or more parts in a finished device, after distribution, for purposes of returning it to the safety and performance specifications established by the original equipment manufacturer (OEM) and to meet its original intended use. Regardless of an entity's self-identified designation as a "servicer" or "remanufacturer," the FDA focuses on the specific activities an entity performs on a particular device. The determination of whether the activities an entity performs are remanufacturing affects the applicability and enforcement of regulatory requirements under the Federal Food, Drug, and Cosmetic Act (FD&C Act) and its implementing regulations. The FDA enforces requirements under the FD&C Act and its implementing regulations on entities engaged in remanufacturing, including but not limited to registration and listing, adverse event reporting, the Quality System (QS) regulation, and marketing submissions.

· Remanufacturing of Medical Devices

Papers and Reports

· Servicing Discussion Paper: Strengthening Cybersecurity Practices Associated with Servicing of Medical Devices: Challenges and Opportunities (June 2021)
· White Paper: Evaluating Whether Activities are Servicing or Remanufacturing (December 2018)
· Servicing Report: FDA Report on the Quality, Safety, and Effectiveness of Servicing of Medical Devices (May 2018)

Workshops

· Public Workshop - Medical Device Servicing and Remanufacturing Activities, December 10-11, 2018
·
· This two-day workshop was intended to publicly discuss the distinction between medical device servicing and remanufacturing activities to better inform the development of a future draft guidance, as well as discuss opportunities for collaboration among medical device servicing and remanufacturing stakeholders.
· Public Docket Comments (No. FDA-2018-N-3741)
·
· Public Workshop - Refurbishing, Reconditioning, Rebuilding, Remarketing, Remanufacturing, and Servicing of Medical Devices Performed by Third-Party Entities and Original Equipment Manufacturers, October 27-28, 2016External Link Disclaimer
·
· This two-day workshop was intended to convene interested stakeholders to discuss regulatory aspects of third party processes including refurbishing, reconditioning, rebuilding, remarketing, remanufacturing and servicing. To promote an understanding of challenges and best practices to mitigate risks associated with these activities, the workshop included FDA remarks, stakeholder perspectives, and four panel discussions based on public docket comments.
· Public Docket Comments (No. FDA-2016-N-0436-001)

Delphi Consulting Group, Houston, Texas 77071-3404
Contact: J. Harvey Knauss, +(832) 675-9281 voice, info@delphiconsulting.com or www.delphiconsulting.com

DCG comments – Medical Device Manufacturing Companies need to make comments regarding this to the FDA. DCG believes that only the original manufacture and/or their contracted representative should be allow remanufacture their medical device.

FDA Hones in on Medical Device Security

Cybersecurity leaders discuss how the agency is implementing new cyber controls to protect medical device integrity. *Sarah Sybert Mon, 06/07/2021 - 12:08*

The Food and Drug Administration is taking a closer look at medical device cybersecurity and countermeasures following supply chain challenges and attacks presented by the COVID-19 pandemic.

"The idea is to be as prepared as possible for the next event. We want to help shorten the time it takes to develop these medical countermeasure devices so that they are available when needed," said FDA Senior Science Health Advisor Heather Agler during FDA's Science Forum last week.

Cybersecurity threats to the health care sector could make medical devices and hospital networks inoperable, thereby disrupting the delivery of patient care. Therefore having medical countermeasure devices in place is critical, Agler said.

FDA is tackling this via threat modeling, which helps identify, analyze and evaluate potential security risks. Threat modeling enables FDA to avoid "gut judgements" on cyber posture and move toward a verifiable security control, said Kevin Fu, acting director for medical device cybersecurity at FDA's Center for Devices and Radiological Health.

"It's the cousin to hazard analysis. The idea is that it's very difficult to make scientific claims about medical device security if a manufacturer doesn't provide a reasonable and reputable threat model specific to the device," Fu said.

Fu outlined three insufficient threat model claims for medical devices: using obscure programming language, relying on past history of never being attacked and placing products on a secure hospital network.

"A good threat model for any device begins with a simple statement: 'We will begin by assuming an adversary controls the network the medical device connects to.' This is a good start to enabling a medical device to stay safe and effective despite anticipated risks of computer security," Fu said.

FDA is also creating software bills of material (SBOM) through the International Medical Device Regulators Forum to help synchronize guidelines and standards internationally.

"This is all about how to get a total product lifecycle to include cybersecurity and bring more consistency across the borders for more certainty for the manufacturing community," Fu said.

SBOMs are growing in importance at the agency, particularly following Biden's executive order on cybersecurity.

"An SBOM is useful to those who develop or manufacture software, those who select or purchase software, and those who operate software," the executive order said. "Those who operate software can use SBOMs to quickly and easily determine whether they are at potential risk of a newly discovered vulnerability."

FDA is also working on a Joint Security Plan, which serves as a total product lifecycle reference guide for developing, deploying and supporting cyber-secure technology solutions in the health care environment.

Throughout 2021, CDRH will develop a strategic roadmap for future medical device security, partner with stakeholders and foster collaborations across industry and government to enhance security as attackers continue to evolve.

"One area I'm hoping to make a good dent in is helping to integrate cybersecurity principles through CDRH's total product life cycle, and help with training and mentoring," Fu said.

Google backs Linux project to make Android, Chrome OS harder to hack

The search giant is working to allow Rust code in the Linux kernel, a major technological and cultural shift after decades using only C. *June 17, 2021 Miguel Ojeda*

Google said Thursday it's funding a project to increase Linux security by writing parts of the operating system's core in the Rust programming language, a modernization effort that could bolster the security of the internet and smartphones.

If the project succeeds, it'll be possible to add new elements written in Rust into the heart of Linux, called the kernel. Such a change would mark a major technological and cultural shift for an open-source software project that's become foundational to Google's Android and Chrome operating systems as well as vast swaths of the internet.

Miguel Ojeda, who's written software used by the Large Hadron Collider particle accelerator and worked on programming language security, is being contracted to write software in Rust for the Linux kernel. Google is paying for the contract, which is being extended through the Internet Security Research Group, a nonprofit that's also made it easier to secure website communications through the Let's Encrypt effort.

Adding Rust modules to the Linux kernel would improve security by closing some avenues for hackers can use to attack phones, computers or servers. Since it was launched in 1991, Linux has been written solely in the powerful but old C programming language. The language was developed in 1972 and is more vulnerable to hacks than contemporary programming languages.

Better security for Linux is good news for everyone but hackers. In addition to the Android and Chrome OSes, Google services like YouTube and Gmail all rely on servers running Linux. It also powers Amazon and Facebook, and is a fixture in cloud computing services.

It isn't clear if Linux kernel leaders will accommodate Rust. Linus Torvalds, the founder of Linux, has said he's open to change if Rust for Linux champions prove its worth. Ojeda has proposed 13 changes needed to allow Rust modules in Linux to get things started.

Google already has taken some early steps to make it possible to use Rust for Linux Android. Getting buy-in at the highest levels of the Linux kernel project means many other software projects could benefit, too.

Google credits the Linux community programmers who began the Rust for Linux project. "The community had already done and continues to do great work toward adding Rust support to the Linux kernel build system," Google said in a blog post.

Rust, which was developed by Firefox maker Mozilla and is now run by the independent Rust Foundation, makes it safer for

software to write to memory. Hackers can exploit memory problems, hiding malicious extra code in out-of-bounds memory areas. Rust checks for those and other problems when programmers are building their software. And it's been the most loved programming language for five years running in Stack Overflow's annual developer survey.

"Rust represents the best alternative to C and C++ currently available," Microsoft's security team concluded in 2019. The team said Rust would have prevented memory problems at fault in 70% of its significant security issues. And because Rust's checks happen while software is being built, the safety doesn't come at the expense of performance when the software is running.

The goal of the Linux on Rust project isn't to replace all of Linux's C code but rather to improve selective and new parts.

"For the foreseeable future we plan to focus on certain security critical components and drivers," said Josh Aas, who runs ISRG's Prossimo project to move critical Internet software to memory safe software. Drivers are operating systems modules that control specific devices like printers, network adapters and graphics chips.

Google isn't placing its only bets on Linux and Rust. It's got its own memory-safe language, Go, and a new operating system called Fuchsia it's begun using in its Nest Hub smart screen.

"Google has a variety of other investments in languages, tools, and platforms," a company spokesman said. "Having multiple solutions to related but not necessarily overlapping problems allows for a cross pollination of good ideas to be reused."

Clinical Outcome Assessments (COAs) in Medical Device Decision Making

At the FDA's Center for Devices and Radiological Health (CDRH), we strive to ensure patients and their care partners remain the focus of our regulatory decision-making process. One way we do that is by encouraging the inclusion of **clinical outcome assessments (COAs)** in the evaluation of medical devices.

What Are Clinical Outcome Assessments?

A clinical outcome assessment (COA) describes or reflects how a person feels, functions, or survives and can be reported by a health care provider or a non-clinical observer (such as a parent), through performance of an activity or task, or by the patient.

There are four types of COAs:

- Patient-reported outcomes (PROs),
- Clinician-reported outcomes (ClinROs),
- Observer-reported outcomes (ObsROs), and
- Performance outcomes (PerfOs).

While each COA focuses on the patient, they provide a different perspective on a patient's health status.

PROs provide information on the patient's health condition as directly reported by the patient, without outside interpretation from anyone. These outcomes are assessed using PRO instruments such as questionnaires, numeric rating scales, or diaries.

ClinROs are reports coming from a trained health-care professional regarding their interpretation of signs or behaviors that can be observed related to a patient's disease or condition.

ObsROs are assessments of observable signs, events, or behaviors related to a patient's health condition as reported by individuals who observe the patient in daily life, like parents or caregivers.

PerfOs are measurements collected when a patient is asked to complete a well-defined, repeatable, and standardized task such as reading an eye chart.

How CDRH Uses COAs in Regulatory Decision Making

For regulatory purposes, high-quality information from COAs can provide valuable evidence for benefit-risk assessments. They can also be used in medical device labeling to communicate the effect of a treatment on patient symptoms and functioning. COAs may be used to determine who is eligible for a clinical study and measure how well the device performs in treating or diagnosing the condition. COAs may also be used to help measure the safety of the device. Evidence from COAs may also be useful to payors and healthcare providers.

COA Case Studies

These case studies highlight the roles COAs can play in clinical investigations supporting medical device submissions. They are not intended to be a comprehensive review of the pivotal clinical studies associated with each submission.

Planning to Incorporate Clinical Outcome Assessments (COAs) in a Regulatory Submission?

If you are interested in incorporating COAs in your regulatory submissions, CDRH has multiple resources to help with selecting, using, developing and modifying appropriate COAs. The FDA has issued guidance documents and discussion guides that may help inform your approach to including COAs in the evaluation of medical devices.

Q-submission: We invite sponsors to discuss their plan to use COAs, including adapting or developing PRO instruments, with CDRH through the Q-submission program. A pre-submission can initiate early discussions with regulatory staff, as described in the guidance document Requests for Feedback and Meetings for Medical Device Submissions: The Q-Submission Program.

Medical Device Development Tools: The Medical Device Development Tools (MDDT) program enables the FDA to qualify tools that medical device sponsors can use in the development and evaluation of medical devices. Qualification means CDRH has evaluated the tool and concurs with available supporting evidence that the tool produces scientifically-plausible measurements and works as intended within the specified context of use. COAs are one type of tool that can be qualified under the MDDT program.

PRO Report: This document provides more detailed information on PROs. It discusses the value of using PROs in regulatory submissions, reimbursement decisions, and clinical practice. Additionally, CDRH efforts and accomplishments to date relating to PROs are highlighted.

PRO Compendium: The PRO Compendium (XLS) lists some, but not all, PRO instruments that have been used and reported in medical device premarket clinical investigations submitted to CDRH. We encourage sponsors interested in using a PRO instrument in a clinical investigation to schedule a pre-submission meeting to discuss their plans.

Contact Us

If you have questions about clinical outcome assessments, email CDRH-PRO@fda.hhs.gov