ORACLE

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

Vol. 25 Issue 7 July 2019

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

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

Keeping up with Counterfeiters: The Battle Against Counterfeit Medical Devices

Steve Ellison, PRISYM ID, examines The Battle Against Counterfeit Medical Devices - article published in MedTech Intelligence

What do you think of when you hear about counterfeit goods—a fake Rolex or a copy designer handbag? Poorly replicated luxury goods cause chaos and generate large profits for counterfeiters, but the real issues lie in plagiarized medical devices, not purses.

It is widely acknowledged that counterfeiting medical devices is a very real and constant threat to patient safety. With the forthcoming implementation of the EU Medical Device Regulation in 2020, there is an increase in demand for more information about product origin. This impending law will have a significant impact throughout the healthcare industry, affecting operations from one end of the supply chain to the other, from manufacturing to distribution.

With anti-Counterfeiting also come effective anti-diversion processes. While we need to ensure the product has not been replicated, we also need to ensure the product has not been removed from the supply chain, tampered with and then re-entered at a different continent, country and/or location.

This column discusses the key issues with counterfeit medical devices and provides recommendations to save money and reduce risk within your supply chain.

Anti-counterfeit measures protect both the manufacturer and the end user. In the life sciences industry and particularly, medical devices, a counterfeit item, when used, puts the patient at risk and impacts the manufacturer through potential damage to reputation, cost of removing these counterfeit goods out of the supply chain and additional effort to prevent further issues occurring. So, it is crucial that medical device manufacturers ensure their packaging, labeling, and supply chain is tight and precisely tracked to the point of use.

The second term we use is anti-diversion. This is to ensure that products that have been developed for a specific market, perhaps with materials that are not allowed in other countries but are authorized for the intended market, validated, compliant and fit for purpose, are not removed from the supply chain, repackaged and sent into a country that should not receive that item. It can be potentially dangerous for patients and is illegal. Therefore, the challenge is to avoid both counterfeit and diverted products.

How can I assure my medical device at the point of use or point of receipt is the right one? Manufacturers have both passive and active methods of clarification and protection.

The Passive Method

Passive methods apply to the packaging. Medical devices usually have three levels of packaging: The primary packaging (pouch), which then goes into a secondary box (product box) and finally packaged into a shipper where there will be multiple products stored in one package.

To avoid counterfeiting, manufacturers can apply deterrents to each of these items of packaging. Whether that be a hologram, UV identification code, 2-D barcode with unique numbering/serialization or hidden text printed using security or magnetic ink. These are not intended as end-user checks but as deterrents to the counterfeiter. A trained person can quickly establish if the product is authentic and can take things further by referencing the unique numbers used in the security marking via an authentication site.

The Active Method

The active method takes the passive method one step further, using various technologies to avert counterfeiting.

A unique serial number or reference number (URN) is a randomized number printed onto the product's packaging and as it's unique, it can be used to define exactly who manufactured the item, where it was manufactured and the country of origin. This type of serialization at the item level is vital in the fight against counterfeiting. Web-based "labeling and data management" solutions can support you in delivering secure printing for mass serialization to protect the product and the consumer. Serialization not only gives the ability to authenticate the product as genuine, but also offers the ability to track product movement throughout the supply chain, improve efficiency and most importantly, protect the end user.

Modern technologies can then use the serialized data in barcode format, which can be scanned at any point throughout the supply chain and checked with online systems to verify its authenticity. If the look-up comes back with no read/duplicate, then we know there is an issue with the product, and it can be rejected out of the supply chain and additional action taken to remove additional counterfeit devices. These methods clearly work, are

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

simple and cost-effective to implement.

Taking things further and linking logistics systems with the serialization detail can give a "smart" active method system that would look for activities and trends based on knowing which serial numbers were assigned to what product, to be sold in a which territory. For example, if a shipment of product with serial numbers assigned to the China market were scanned at a customer site in South America, this would be captured as a diverted product and flagged up to the manufacturer/supplier accordingly to engage and investigate.

It is therefore a combination of both passive and active methods that ensure true safety of counterfeiting items.

International Challenges

Destination labeling or just-in-time labeling is where products are predominantly manufactured with a single language printed label along with the product name and production variables. Traditionally, a product label would carry four or five additional languages on the packaging, along with an Instructions for Use (IFU) booklet that would contain every language where the product is approved for use. By law, the manufacturer has to print and ship the product with all the languages that may use it, which could be anything up to about 60 different languages, so region-specific labeling takes place to lessen the quantity of languages used on the label, which may take the number used, back down to five or six.

In the medical device industry today, consumers want the label to show just their local language or languages. With just-in-time labeling, you can develop a product label solution linked to orders received and use the end destination to drive the language(s) to be printed on the label and rather than use a pre-printed, large and expensive IFU booklet, print a single sheet containing the same languages as the label at the same time as the label is printed. This approach offers great flexibility, shorter time to market and huge cost savings linked to the elimination of the expensive IFU booklets.

If an item located in a regional distribution center needs to be redirected to a different market to that originally packaged and labeled, it will require a degree of repackaging, and this activity may be prone to risk of a counterfeited product being introduced into the supply chain. In any re-packing and re-labeling operation away from the manufacturer's site and outside the manufacturer's control, the important serialization data and other security measures can be lost, not replicated correctly or replaced with incorrect/cloned data to support the counterfeiter's operation. It is at these smaller distribution hubs or sites where the re-packing takes place and the risk is highest for the introduction of counterfeited good into the supply chain.

By nature, if that product is labeled in Spanish and English, but needs to go to China, you would normally take off all the language-specific packaging and repackage with the corresponding language(s). But with the removal of these discrete codes, serialization and barcodes, we are removing and throwing away imperative security measures. Medical device companies are now installing controlled third-party print stations in warehouses to ensure local distributors are repackaging and re-labeling the product in a controlled way, the local language labels retain the serialization data, are printed with the local language approved design and format and any tracked field such as the unique serial number is carried over and the re-labeling event written back to the manufacturer's global audit log.

Regional redirection then becomes part of the supply chain infrastructure and controlled accordingly. You will still be able to see the re-labeled item in the system, validated as authentic at a checkpoint, and re-labeled to the right destination market supported by the track and trace audit log. So, if re-labeling is taking place, with the right holistic approach and right controls, risk of counterfeit items entering the supply chain is reduced. Ideally, if you implement a just-in-time destination labeling solution at the point of manufacture, you can remove the need to re-label the solution out in the field and ensure it is securely delivered to the right destination in a shorter time frame.

Conclusion

Organizations need to make sure that they put into practice the correct systems and processes that can support them in meeting global standards and country-specific requirements now and in the future. Implementing a fit-for-purpose validated labeling solution with in-built serialization capabilities, which can provide very high volumes of unique, secured and "intelligent" serial numbers for this process would therefore be vital.

Control your label, its design, and the data to reduce risk. If you don't have control of these three things, it's likely that counterfeiting can creep in. Keeping up with counterfeiters in the life sciences industry is no easy task, but patients' lives depend on it.

Steve Ellison, VP European Sales, PRISYM ID

Steve has spent over 24 years working with coding and labelling solutions and for the last four years he has been running the European Sales Consultancy team, promoting and implementing PRISYM ID's world class labelling software solutions.

During his time with PRISYM ID, he has observed many changes within the industry including significant tightening of regulations, the challenges of globalization, implementation of directives such as UDI and EU MDR.

FDA Debates Framework for AI-Based Medical Devices

A new approach to premarket review for AI and machine learning–driven modifications to medical devices is underway at the federal agency (FDA).

Gienna Shaw is an independent journalist with more than 25 years of experience as a writer and editor. She specializes in business, technology and healthcare.

The FDA is crafting **a new regulatory framework** to promote the development of safe and effective medical devices powered by advanced artificial intelligence algorithms. The agency sees promise in adaptive AI and machine learning technologies, noting they "have the potential to adapt and optimize device performance in real time to continuously improve healthcare for patients."

Under the current rules, any changes made in medical devices' software requires FDA approval. But that rule would be burdensome for companies that make adaptive software powered by AI and machine learning because **the software is continuously changing** — and improving — as it gathers data.

***MORE FROM HEALTHTECH**: Three ways to manage risks posed by connected medical devices*.

Cybersecurity and Medical Devices

The U.S. Food and Drug Administration is warning patients and health care providers that certain Medtronic MiniMed insulin pumps are being recalled due to potential cybersecurity risks and recommends that patients using these models switch

their insulin pump to models that are better equipped to protect against these potential risks. To date, the FDA is not aware of any confirmed reports of patient harm related to these potential cybersecurity risks.

The potential risks are related to the wireless communication between Medtronic's MiniMed insulin pumps and other devices such as blood glucose meters, continuous glucose monitoring systems, the remote controller and CareLink USB device used with these pumps. The FDA is concerned that, due to cybersecurity vulnerabilities identified in the device, someone other than a patient, caregiver or health care provider could potentially connect wirelessly to a nearby MiniMed insulin pump and change the pump's settings. This could allow a person to over deliver insulin to a patient, leading to low blood sugar (hypoglycemia), or to stop insulin delivery, leading to high blood sugar and diabetic ketoacidosis (a buildup of acids in the blood).

"The FDA urges manufacturers everywhere to remain vigilant about their medical products—to monitor and assess cybersecurity vulnerability risk, and to be proactive about disclosing vulnerabilities and mitigations to address them. This is part of the FDA's overall effort to collaborate with manufacturers and health care delivery organizations—as well as security researchers and other government agencies—to develop and implement solutions to address cybersecurity issues throughout a device's total product lifecycle," said Suzanne Schwartz, M.D., MBA, deputy director of the Office of Strategic Partnerships and Technology Innovation and acting division director for All Hazards Response, Science and Strategic Partnerships in the FDA's Center for Devices and Radiological Health. "While we are not aware of patients who may have been harmed by this particular cybersecurity vulnerability, the risk of patient harm if such a vulnerability were left unaddressed is significant. The safety communication issued today contains recommendations for what actions patients and health care providers should take to avoid the risk this vulnerability could pose. Any medical device connected to a communications network, like Wi-Fi, or public or home Internet, may have cybersecurity vulnerabilities that could be exploited by unauthorized users. However, at the same time it's important to remember that the increased use of wireless technology and software in medical devices can also offer safer, more convenient, and timely health care delivery."

The recalled pumps are Medtronic's MiniMed 508 insulin pump and MiniMed Paradigm series insulin pumps. Medtronic is providing alternative insulin pumps to patients with enhanced built-in cybersecurity capabilities. In the U.S., Medtronic has identified 4,000 patients who are potentially using insulin pumps that are vulnerable to this issue. In addition, Medtronic is working with distributor partners to identify additional patients potentially using these pumps.

The affected devices wirelessly connect to both the patients' blood glucose meter—which measures a patient's blood glucose levels at one point in time—and continuous glucose monitoring system—a sensor and transmitter that track a patient's glucose levels throughout the day.

The remote controller and CareLink USB, a thumb-sized wireless device that plugs into a computer, are used with the affected insulin pumps. A patient can use the remote controller to send insulin bolus (dosing) commands to the insulin pump remotely and can use the CareLink USB to download data about their glucose levels from their insulin pump to monitor their own progress and share it with their health care provider.

The U.S. Food and Drug Administration is warning patients and health care providers that certain Medtronic MiniMed insulin pumps are being recalled due to potential cybersecurity risks and recommends that patients using these models switch their insulin pump to models that are better equipped to protect against these potential risks. To date, the FDA is not aware of any confirmed reports of patient harm related to these potential cybersecurity risks.

The potential risks are related to the wireless communication between Medtronic's MiniMed insulin pumps and other devices such as blood glucose meters, continuous glucose monitoring systems, the remote controller and CareLink USB device used with these pumps. The FDA is concerned that, due to cybersecurity vulnerabilities identified in the device, someone other than a patient, caregiver or health care provider could potentially connect wirelessly to a nearby MiniMed insulin pump and change the pump's settings. This could allow a person to over deliver insulin to a patient, leading to low blood sugar (hypoglycemia), or to stop insulin delivery, leading to high blood sugar and diabetic ketoacidosis (a buildup of acids in the blood).

"The FDA urges manufacturers everywhere to remain vigilant about their medical products—to monitor and assess cybersecurity vulnerability risk, and to be proactive about disclosing vulnerabilities and mitigations to address them. This is part of the FDA's overall effort to collaborate with manufacturers and health care delivery organizations—as well as security researchers and other government agencies—to develop and implement solutions to address cybersecurity issues throughout a device's total product lifecycle," said Suzanne Schwartz, M.D., MBA, deputy director of the Office of Strategic Partnerships and Technology Innovation and acting division director for All Hazards Response, Science and Strategic Partnerships in the FDA's Center for Devices and Radiological Health. "While we are not aware of patients who may have been harmed by this particular cybersecurity vulnerability, the risk of patient harm if such a vulnerability were left unaddressed is significant. The safety communication issued today contains recommendations for what actions patients and health care providers should take to avoid the risk this vulnerability could pose. Any medical device connected to a communications network, like Wi-Fi, or public or home Internet, may have cybersecurity vulnerabilities that could be exploited by unauthorized users. However, at the same time it's important to remember that the increased use of wireless technology and software in medical devices can also offer safer, more convenient, and timely health care delivery."

The recalled pumps are Medtronic's MiniMed 508 insulin pump and MiniMed Paradigm series insulin pumps. Medtronic is providing alternative insulin pumps to patients with enhanced built-in cybersecurity capabilities. In the U.S., Medtronic has identified 4,000 patients who are potentially using insulin pumps that are vulnerable to this issue. In addition, Medtronic is working with distributor partners to identify additional patients potentially using these pumps.

The affected devices wirelessly connect to both the patients' blood glucose meter—which measures a patient's blood glucose levels at one point in time—and continuous glucose monitoring system—a sensor and transmitter that track a patient's glucose levels throughout the day.

The remote controller and CareLink USB, a thumb-sized wireless device that plugs into a computer, are used with the affected insulin pumps. A patient can use the remote controller to send insulin bolus (dosing) commands to the insulin pump remotely and can use the CareLink USB to download data about their glucose levels from their insulin pump to monitor their own progress and share it with their health care provider.

[SIC] You may become tired of hearing about this but there are evil people in the world. If a device has 'wireless' features steps must be taken to harden it from possible cyber-attacks.