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

ORACLE

NEWSLETTER FROM DELPHI CONSULTING GROUP (DCG)
An Internet Based Medical Device Regulatory Service, www.delphiconsulting.com
Established 1987

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.

Issue 252 November, 2015

Software as a medical device: How HIPAA security paves way for FDA classification

No matter the application’s purpose, one that is developed or tweaked under FDA guidelines is one ready for prime time. Broadly defined, software as a medical device is any application used by providers to make clinical decisions. An increasing number of applications are now officially designated as FDA-regulated devices. Is it worth it to pursue this classification for your own software?

If your objective is to make it an indispensable tool in the healthcare and life sciences industries, there is a decided market advantage to entering the regulated medical device arena. What's more, work you have done to date to achieve compliance with another set of controls – the HIPAA Security Rule – can be applied to obtaining the FDA classification.

On that note, be aware that the FDA has three tiers of classification for medical devices, each based on intended use of the application and the risk the application poses to patients or users.

This article is concerned with FDA Class I, the tier reserved for low-risk devices, and therefore, subjected to the least amount of regulation. All Class 1 devices must, however, conform to certain requirements, including annual registration with the FDA, careful product labels and descriptions on both the product and accompanying sales and marketing literature, and other regulations.

The upside of FDA scrutiny there are a number of reasons – all good ones – why software companies would willingly jump through the necessary hoops to obtain FDA classification.

First, large integrated health networks increasingly need FDA classification for the applications they use to make medical decisions. It makes life a lot easier for them, especially from a legal standpoint, if these apps are cleared for FDA approval.

Healthcare is also entering an unprecedented collaborative era, with a proliferation of joint projects concerned with testing new innovations and technologies. The market for a promising new product could be bigger with FDA classification.

There's also the matter of software taking an ever more important role in healthcare. From analytics to radiation dose monitoring, healthcare today relies on a broad range of applications. For many of these apps, FDA classification is or will become a mandate. Vendors that get ahead of this now will be better positioned than those that have to rush to catch up.

Some may be wondering if this includes consumer-focused apps, such as personal health tracking and coaching products. As it happens, in early 2015 the FDA released a report of exempt mobile apps. However, should vendors market or intend these apps as a means for diagnosing, curing or preventing diseases, the FDA will consider them non-exempt from regulation.

HIPAA compliance – a springboard to FDA Class I

No matter the application's purpose, one that is developed or tweaked under FDA guidelines is one ready for prime time. But how much work are vendors really looking at to get there? No doubt, even for Class I, the requirements are rigorous.

The good news is that an application designed to comply with the technical safeguards of the HIPAA Security Rule has a head start for some FDA Class 1 domains. Both sets of controls address configuration management, for example, along with monitoring and physical environmental security. In addition, adherence to security and privacy will only grow in importance as hackers increase their targets to include medical devices and medical device software.

But what if you suspect your application isn't secure at all, or lacks basic privacy features? How do you step up your security and privacy game, without making the road to FDA classification even longer? The quickest – and increasingly safest – route is to bring in expertise.

Many healthcare organizations and the vendors who serve them are turning to "cloud" managed services partners for a broad set of security and privacy services. These can span from an initial risk assessment of the IT infrastructure that houses your applications, to privacy impact and software development lifecycle assessments, to ongoing, managed hosting of this infrastructure within a cloud environment that exceeds HIPAA, GAPP and other security and privacy controls.

It should be emphasized that vendors need to secure their applications regardless of whether or not they obtain FDA classification. There are too many breaches today and too much at stake when these breaches occur. That said, if you're ready to pursue FDA Class I, migrating your app to a HIPAA-compliant managed cloud can jump start your path. ☺

FDA orders postmarket studies from trio of duodenoscope makers as 'superbug' scare continues

October 6, 2015 | By Stacy Lawrence

The three manufacturers that market duodenoscopes in the U.S.--Olympus America, Fujifilm Medical Systems and Hoya through its Pentax division--have all been required by the FDA to submit postmarket surveillance plans to the agency within 30 days. This comes after all three received warning letters from the agency in August and an FDA committee panel took up the same issue in May.

It's just the next step in a years-long saga as the FDA works to prevent the spread of infections, sometimes of antibiotic-resistant bacteria, between patients because reusable duodenoscopes have been ineffectively cleaned. Other types of reusable endoscope have also been called into question as potential sources of infection, since these devices uniformly have difficult-to-clean joints. Meanwhile, industry and hospitals are turning to a variety of solutions including novel cleaning and sterilization approaches and disposable device covers.

The postmarketing data is intended to offer a means for the FDA to better understand precisely how the infections are still occurring, despite cleaning methodologies that have been scrutinized by the FDA and the companies as well as hospitals and healthcare providers themselves.

The proposals must include detailed plans on how the manufacturer will evaluate how well healthcare providers are following instructions on the cleaning and disinfection of duodenoscopes between patients. They are also intended to offer a better tool for assessing the rate of contamination by duodenoscopes in clinical use.

"This is a significant step in the effort to combat infections spread through duodenoscopes," said Dr. William Maisel, deputy director for science and chief scientist at the FDA's Center for Devices and Radiological Health, in a statement. "The FDA has undertaken an in-depth investigation into the factors that may play a role in infection transmission associated with duodenoscopes, and is now requiring manufacturers to study the devices in the clinical setting where they are being used."

The postmarket study plans must address the following three questions, the agency said:

- "Are user materials, such as user manuals, brochures and quick reference guides included in the manufacturers' duodenoscope labeling and instructions for use, sufficient to ensure user adherence to the manufacturers' reprocessing instructions?
- After use of the manufacturer's validated reprocessing instructions, what percentage of clinically used duodenoscopes remain contaminated with viable microorganisms?
- For devices that remain contaminated after use of the manufacturers' labeled reprocessing instructions, what factors contribute to microbial contamination and what steps are necessary to adequately decontaminate the device?"

Concluded Maisel, "These studies will provide critical information about the effectiveness of current reprocessing instructions and practices that may provide additional information to inform the FDA's actions to protect the public health and help reduce the risk of infections."

- here is the FDA statement provide assurance of safety. ☺

Medicare is in the dark on device data

By Cybele Bjorklund

This fall, the medical device safety effort Congress kicked off in 2007 will reach another milestone. As of September 24, 2015, all new, implantable life-sustaining and life-saving medical devices will bear a scannable unique device identifier (UDI)—similar to a barcode like one you'd find on a cereal box—that identifies a device's make and model. Because the devices implanted in patients are critical clinical information, collecting these codes in health insurance claims databases would allow manufacturers, researchers, and regulators to track performance and identify safety issues.

A spate of high-profile medical device recalls in the mid-2000s spurred Congress to create the UDI tracking system. Now, after years of legislating and rulemaking, manufacturers are doing their part by affixing UDI codes to their products.

But despite private sector compliance, Congress's intent in creating the UDI system—improved patient safety—has not yet been met. Until we collect this information and integrate it fully into the healthcare system, our medical device data will remain as outdated as paper files and faxed prescriptions.

Device-specific information remains one of the black boxes of health data. In recent years, the American healthcare system has embarked on a digital revolution, and the nation's largest payer, Medicare, has led the way with its rich claims information. A recent much-heralded data release shared unprecedented amounts of information about the drugs and procedures for which Medicare pays. There are countless applications for these data, including product development, creating new payment models, identifying efficiencies within current systems, and analyzing outcomes.

However, the big piece missing from that data is device-specific information. Although Medicare can tally basic information about device-related procedures--how many are performed and how much we spend--we simply have no way of knowing which specific devices are used, because that data is not being collected.

That means the Centers for Medicare & Medicaid Services (CMS), which administers the Medicare program, lacks key information about its single most commonly reimbursed inpatient procedure—joint replacement, which accounted for almost 450,000 admissions and $7 billion of spending in 2013. Just last month, CMS recognized joint replacement as a key opportunity to improve quality and control spending when it announced a major initiative to bundle payments for care associated with these procedures, thus providing an incentive for better clinical coordination and linking reimbursement with the patient outcomes.

While bundling has the potential to be a transformative development in payment reform, policymakers need to be able to look "under" the bundle to see where the savings are coming from. . As long as CMS and other interested stakeholders cannot obtain information on the specific devices used in procedures, policy makers will stay in the dark on a key variable that can have a significant effect on the quality and cost of care.

Claims data can also be a powerful tool for identifying problems in health care and developing solutions. The FDA's Sentinel Initiative, which relies on claims data to track drug performance, has seen early success: At least 70 peer-reviewed articles have relied on data from the five-year-old project. Because of Sentinel's accomplishments, Congress instructed FDA to expand the program to track devices, too. But this is a near-impossible task unless Sentinel has access to UDI data in claims.

All that is needed to rectify the situation is a single change to the Medicare claims form. Conveniently, the form is already being updated, making the inclusion of UDIs a no-brainer. Unfortunately, CMS is opposing this change, which puts the organization at odds with FDA and many independent experts. The agency cites the cost of the entire claims form overhaul—which will happen regardless—as justification to avoid collecting UDI data.

As the baby boomer generation ages, medical devices will become even more significant drivers of healthcare spending, and their performance will affect the health of more and more Americans. There is no excuse for allowing inertia to trump Congress' intent by preventing us from harnessing this data to improve patient safety, transparency and accountability.

CMS should include UDI information on the claim form during this round of revisions. If it continues to resist, Congress should step in and require integration of UDI codes so the system can fulfill its promise. The time has come to fill this gaping hole in Medicare data. You have to love it. 💣

In the US
November is the month
we change our clocks back to real time. Time that fits with the position of the earth and sun as it should be.

Daylight Saving Time is Dumb!