Medtech Insight
Issue 23
medtech.pharmamedtechbi.com
Pharma Intelligence Informa
December 19, 2016


Shutterstock: igorstevanovic

QUALITY SYSTEM INSPECTION TECHNIQUE:

Do FDA Investigators Play Fast And Loose?

SHAWN M. SCHMITT shawn.schmitt@informa.com

Two authors of US FDA's Quality System Inspection Technique say too many agency investigators aren't always following the auditing approach when conducting facility inspections, often catching device manufacturers by surprise as they manage onsite FDA audits.

The claims come as one of the authors – Tim Wells – says QSIT is outdated and desperately needs a facelift; he is in the process of creating his own updated version of the document for use by companies as they internally audit.

Yet other industry experts say it isn't unreasonable for investigators to stray slightly from QSIT and they believe the aging technique is still relevant. And FDA, for its part, maintained in a Nov. 22 email to *Medtech Insight* that QSIT is indeed used during the vast majority of inspections.

But Wells isn't so sure. "Yes, there are investigators that follow QSIT, but let me assure you that there are way more investigators, in greater numbers, that simply don't follow the technique," he said. Wells is a former longtime CDRH staffer who led the Quality System Inspections Reengineering Team that devised QSIT. He spoke with *Medtech Insight* during separate Sept. 16, Oct. 3 and Nov. 14 interviews.

The 108-page QSIT manual directs investigators to look for particular information on a range of quality-related documents and records, among other things. QSIT was penned in the late 1990s and piloted with industry between October 1998 and February 1999. The technique officially took effect on Oct. 1, 1999, and has not been changed since, despite FDA's insistence that it routinely reviews such guidance documents for possible revision.

QSIT is designed to make sure that investigators look at the most important compliance issues and ask pertinent questions linked to four major quality system subsystems: management controls, corrective and preventive action (CAPA), design controls, and production and process controls.

No other commodity – not drugs, not dietary supplements, not even foods – requires such a prescriptive inspectional technique, making medical devices unique when it comes to agency auditing.

QSIT is used for abbreviated FDA Level 1 inspections, which covers CAPA plus only one other quality system subsystem; the investigator can choose between production and process controls, or design controls. It is also used for traditionally less

CONTINUED ON PAGE 17

FROM THE EDITORS OF: **THE GRAY SHEET, CLINICA, START-UP** AND **MEDTECH INSIGHT NEWSLETTER**

Pharma intelligence

informa

Intelligence with a Global Perspective

The Premier Resource In The Life Sciences Industry

- Biomedtracker
- Datamonitor Healthcare
- In Vivo
- Meddevicetracker
- Medtrack
- Medtech Insight
- Pink Sheet
- Pharmaprojects
- RxScorecard
- Scrip
- Sitetrove
- Trialtrove

Pharmaintelligence.informa.com

The next issue will be January 2, 2017. For online access please contact customer care at 888-670-8900 or clientservices@pharmamedtechbi.com

explore more:

exclusive online content

Medtech and DoJ
http://bit.ly/29zivFF
A snapshot of US Department of Justice medtech settlements, pleas and convictions.

Presentation: EU reg reforms
http://bit.ly/29zivFF
Medtech Insight's Amanda Maxwell provided a deep-dive look at the new Medical Device and IVD Regulations coming soon to the EU during a recent presentation at the Drug/Device Combination Products meeting in Berlin, organized by KNect365, an Informa business.

November M&As hit low
http://bit.ly/2h0EfgL
M&A deal activity dropped dramatically in November with a mere six deals in the medtech industry, making it the weakest month of the year so far.

CMS insists on CED for spine procedure
http://bit.ly/29zivFF
The US Medicare agency said it will stick with its trial-limited coverage-with-evidence-development policy for percutaneous image-guided lumbar decompression, but will expand the accepted study types.

Device Week
http://bit.ly/2gJa4ia
Our weekly podcast, where *Medtech Insight* journalists discuss topics they are covering that impact the device and diagnostics sector.

medtech.pharmamedtechbi.com

inside:

Medtech insight

DAVID FILMORE @MEDTECHDAVID
david.filmore@informa.com
TINA TAN @MEDTECHTINATAN
tina.tan@informa.com
SHAWN M. SCHMITT @MEDTECHSHAWN
shawn.schmitt@informa.com
REED MILLER @MEDTECHREED
reed.miller@informa.com
AMANDA MAXWELL @MEDTECHAMANDA
amanda.maxwell@informa.com
SUE DARCEY @MEDTECH_INSIGHT
sue.darcey@informa.com
FERDOUS AL-FARUQUE @MEDTECH_DANNY
danny.al-faruque@informausa.com
ELIZABETH ORR @ELIZABETHJORR
elizabeth.orr@informa.com
CATHERINE LONGWORTH @MEDTECHCATE
catherine.longworth@informa.com
ASHLEY YEO @ASHLEYPYEO
ashley.yeo@informa.com
MAUREEN KENNY @SCRIPREGMAUREEN
maureen.kenny@informa.com
NEENA BRIZMOHUN @SCRIPREGNEENA
neena.brizmohun@informa.com
VIBHA SHARMA @SCRIPREGVIBHA
vibha.sharma@informa.com
JANET HANIAK SENIOR DESIGNER
GAYLE REMBOLD FURBERT DESIGN SUPERVISOR
RICHARD FAINT HEAD OF MEDTECH
richard.faint@informa.com
PHIL JARVIS MANAGING DIRECTOR

Editorial office:
52 Vanderbilt Avenue, 11th Floor, New York, NY 10017
phone 240-221-4500, fax 240-221-2561

CUSTOMER CARE:
1-888-670-8900 OR 1-908-547-2200
FAX 646-666-9878
clientservices@pharmamedtechbi.com

▶ join the conversation

We are tweeting, chatting, liking and sharing the latest industry news and insights from our global team of editors and analysts — join us!

@Medtech_Insight

Interview: Where Do New Reprocessing Rules Leave EU?

AMANDA MAXWELL amanda.maxwell@informa.com

Reprocessing of single-use devices was one of the most contentious subjects when it came to drafting the EU Medical Devices Regulation, which are set to be adopted next year, and it was one of the subjects that contributed to the ongoing delays in reaching agreement in 2015 and earlier in 2016.

EU member states could not agree about whether reprocessing should be permitted, and the European Council, made up of member state representatives, could not agree with the European Parliament. Once the Council and Parliament reached agreement earlier this year, the European Commission could not agree with either of the other institutions but finally gave way to a compromise allowing a political agreement to be put forward on the MDR in June.

> "Frankly, as SUD remanufacturers now need to meet all the same MDR requirements as any other manufacturer and await member states to affirmatively opt in, the standard for SUD remanufacturing is now higher than it is for most manufacturers."

So, after all the debate, what is the path forward for this practice that advocates say saves money and improves the environment, while skeptics point to as a safety hazard?

To find out, *Medtech Insight* interviewed Dan Vukelich, president of the global Association of Medical Device Reprocessors (AMDR). He says new requirements will bring about far-reaching changes in the EU.

Medtech Insight: Can you explain what the future rules for the reprocessing of single-use devices will be under the forthcoming Medical Devices Regulation?

Dan Vukelich: Original equipment manufacturers, third-parties or even health-care providers like hospitals who reprocess single-use devices (SUD), will be subject to the medical device manufacturing requirements of the European Medical Device Regulation (MDR) once fully implemented.

This is somewhat like the regulatory approaches adopted by the US FDA in 2000 and subsequently in Germany, Canada, Australia, the framework currently under consideration in Japan, and consistent with recently released recommendations from the World Health Organization.

On a broad level, after implementation, any entity that reprocesses an SUD for reuse needs to meet the full set of manufacturing requirements as outlined in the MDR – like any other manufacturer.

However, unlike any other CE-marked device meeting the requirements of the MDR, reprocessed devices must also be permitted by the individual member state markets. This means member states must affirmatively "opt in" to allowing reprocessed or remanufactured devices on their market.

So, the final MDR on SUD reuse is not the single, harmonized EU approach we and many others had hoped for, but it sets the minimum standards going forward.

Why do you say that the European approach in the final MDR is "somewhat consistent" with the manufacturer treatment of SUD reuse as adopted by other international regulators?

Vukelich: I say that because, in addition to the "opt in" requirements noted above, the reprocessing section of the regulation, currently Article 15*, also creates a "carve out," as urged by Germany, for in-house (hospital) reuse of SUDs. This article outlines the minimum requirements for hospital reuse and the European Commission is to come up with further "common specifications." This is unlike any other manufacturer regulatory paradigm for SUD reprocessing that has emerged internationally as all other countries have held all reprocessors to the same manufacturer standard.

How do the new MDR rules differ from the current regulation of reprocessing around Europe?

Vukelich: Currently, the reuse of SUDs is subject to member state rules and they vary considerably.

Germany has had a stringent regulatory scheme for all device reuse in place since 2002 under the Recommendation of the Commission for Hospital Hygiene and Infection Control at the Robert Koch Institute in Germany [the KRINKO guidelines]. France bans SUD reuse altogether.

The UK recently adopted new guidance clarifying they continue to discourage hospital reuse of SUDs, but they allow CE-marked, "remanufactured" SUDs on the UK market – consistent with the EU MDR approach.

Otherwise, most member states have no formal policy. And, data collected by our association, the Association of Medical Device Reprocessors, AMDR, indicates that SUD reuse of some devices is taking place in many EU member state hospitals, including in countries with bans on reprocessing.

We think opting into the EU MDR's manufacturing paradigm for SUD reprocessing is an opportunity to stop inappropriate, un-validated, in-house reprocessing of SUDs and usher in only safe, regulated, CE-marked reprocessed, or rather, remanu-

CONTINUED ON PAGE 14

Abbott Steps Up Effort To Abandon Alere Deal

ELIZABETH ORR elizabeth.orr@informa.com

The latest salvo in **Abbott Laboratories Inc.**'s effort to back out of its planned acquisition of diagnostics firm **Alere Inc.** came in the form of a complaint asking a Delaware court to cancel the merger. The suit could be enough to cancel the merger, analysts suggest, but Alere is not backing down from its push to close the deal.

Abbott agreed to buy Alere for $5.8bn on Jan. 30, 2016. But the merger landed on shaky ground soon after that as a series of financial and regulatory missteps by Alere came to light. Alere filed its 2015 annual report five months late, was hit by a major recall, and has been served two criminal subpoenas related to possible Medicare and Medicaid fraud. In addition, Alere's diabetes division has been blocked from billing government health-care programs.

After Abbott took initial steps to back away from the deal, Alere sued in August to compel Abbott to finalize the merger. That case was set to go to trial in January.

Abbott's new suit, which was filed Dec. 7 in Delaware Chancery Court, claims that Alere's troubles make finalizing the merger impossible. The merger agreement allowed Abbott to terminate the agreement if adverse events changed Alere's long-term prospects.

"Alere is no longer the company Abbott agreed to buy 10 months ago," said Abbott spokesman Scott Stoffel. "These numerous negative developments are unprecedented and are not isolated incidents brought on by chance. We have attempted to secure details and information to assess these issues for months, and Alere has blocked every attempt. This damage to Alere's business can only be the result of a systemic failure of internal controls, which combined with the lack of transparency, led us to filing this complaint."

Alere, meanwhile, says the suit is without merit and that it will continue to attempt to compel the merger. "As Abbott well knows, none of the issues it has raised provides it with any grounds to avoid closing the merger," the company said in a statement.

The total weight of the challenges cited by Abbott may be enough to cancel the agreement even if each individual factor wouldn't be, Deutsche Bank research analyst Kristen Stewart said in a Dec. 7 research note. The suit didn't change Deutsche Bank's recommendation for investors to purchase Abbott stock.

Abbott's complaint is sealed, although a redacted version should be available later this month.

Published online 12/7/16

Device-Makers Have Amped Up Defenses Against Hackers

FERDOUS AL-FARUQUE danny.al-faruque@informa.com

While potential medical device vulnerabilities and hacks against health-care systems have taken headlines over the past year, manufacturers have been bulking up their efforts to defend the integrity of their products and their reputation.

The first step in understanding where the threat may be coming from depends on the type of connected medical device that may be vulnerable to an attack. On one end of the spectrum: large devices, such as imaging machines, that are used in hospital settings and rely on standard Transmission Control Protocol/Internet Protocol (TCP/IP), and commercial platform operating systems such as Microsoft Windows. On the other end are smaller devices, including implantables such as pacemakers and implantable insulin pumps that often use proprietary software and protocols.

Axel Wirth, a health-care solutions architect with cybersecurity firm Symantec, says there are various approaches hackers can use including tools-based and experience-based approaches, and sometimes it requires a little detective work to figure out how to break into a device.

There are vulnerability and exploit scanner tools that hackers often have access to that can potentially be used to break into devices if the hacker has advanced knowledge of the relevant vulnerabilities such as reliance by a device on an outdated operating system or a network stack. With that knowledge, they can come up with an attack strategy. According to Wirth, this type of attack is typically used on larger devices that employ commercial software.

"If you get to the other end of the spectrum with proprietary devices, there it becomes more of a detective-type of approach where you really need to start to understand the device, how

CONTINUED ON PAGE 10

Health Enterprise East Introduces New £1.5m Early-Stage Medtech Fund

CATHERINE LONGWORTH catherine.longworth@informa.com

The UK National Health Service's innovation hub Health Enterprise East (HEE) has launched a new £1.5 million award scheme called MedTech Accelerator, to support early-stage medtech innovation. Awards of between £15k and £125k will be up for grabs to develop ideas for technology to improve patient care.

HEE was set up twelve years ago by the Department of Health to support NHS staff in developing ideas for products or services into commercial opportunities. It provides professional advice on patens and intellectual property protection and also provides funding for development work to show proof of concept and support in finding the most appropriate route to market.

Anne Blackwood
CEO of HEE

Photo credit: Health Enterprise East (HEE)

Since 2003, it has received around 200 innovation disclosures a year from NHS staff and successfully exited two of its portfolio companies. Anne Blackwood, CEO of HEE told *Medtech Insight*: "Around 5 years ago we had a plastic surgeon who was doing otoplasty surgery [an operation to pin back and correct prominent ears on a child]. His young patient died on the operating table under general anesthetic. He thought - why does that have to happen to someone just because they want corrective surgery? So he came up with a new idea for treatment."

The surgeon pioneered the minimally invasive treatment called *earFold* with a small implantable device made from a metal alloy which is specifically designed to retain a preset shape. The device is inserted in the back of the ear through a 10-minute outpatient appointment carried out under a local anesthetic. Over the course of three to six months, the patient's cartilage then reforms around the implant. "The procedure doesn't require a 24-hour patient stay so it is cheaper for the NHS and is safer as it requires no general anesthetic. So it's an example of a simple innovation that ticks all the boxes in terms of improving patient care and is cheaper and safer," said Blackwood.

HEE helped the surgeon patent the idea and set up studies to trial the treatment. They then helped set up a spin out company Northwood Medical Innovation which attracted £1m of investment. In 2013, earFold was launched onto the market at the Royal Free Hospital and in 2015, the company was bought by global pharmaceutical **Allergan PLC**.

The organization also provides services to SMEs within the medtech industry, providing access patients, clinicians and stakeholders within the system to understand who the customer might be for a new product. It also works with European and global companies to understand foreign markets but has particular knowledge of the UK. Blackwood said: "Because of our deep relationships with the NHS and because we work with 30 NHS organizations, we understand the front door to the NHS and the NHS as a market. We see ourselves as an organization that is a bridge between the NHS and industry."

HEE's new Medtech Accelerator grant is designed to fund early stage activity such as market research, patenting technology or early stage technical feasibility. "We're also working on a second investment fund to be launched early next year which will allow us to create more spin out companies by having seed funding to do the first round of investment into the company. This fund will be for later stage technology, as more money is required for clinical trials but we want to develop a suite of financial offerings to support medtech innovation."

In the coming year, HEE will provide assistance to a growing number of NHS organizations. "The medical technology market is growing globally and will continue to do so as healthcare needs are growing and I think the market is increasing," Blackwood said. "But the NHS is going through some difficult times and certainly morale in the service is at its lowest point. One of the rewarding things we can do at HEE is supporting people away from the day to day pressures of delivering the job. I think there's no shortage of innovation in the NHS and no shortage of market if you can bring together all the right elements, which is what we aim to do."

Published online 12/12/16

HemoCue Promotes Cloud-Based Anemia Diagnosis Solution For India

PENELOPE MACRAE

Swedish diagnostics giant **HemoCue AB** believes it has a valuable cloud-based diagnostic and analytical tool that can significantly lower the incidence of anemia in India, home to the highest number of cases of the disorder in the world.

Anemia, which occurs when the blood doesn't carry enough oxygen, most often stems from iron deficiency. But it can also be caused by parasitic infections and other conditions, and it is mainly rooted in poverty. The condition affects nearly half of all Indian women, a quarter of all men, and 79% of children aged 6-59 months, according to HemoCue.

"The problem of anemia is generational – an anemic woman has an anemic child and it carries on; it's a vicious cycle," HemoCue president Bjorn Christ told *Medtech Insight* in New Delhi, where the company launched its new real-time diagnosis and analysis system.

The costs from anemia are heavy, both in human and economic terms, as it causes one-fifth of maternal deaths. During pregnancy, anemia also raises the chances of fetal deaths and underweight babies. In children, it affects cognitive and motor skills. The disease can also have big economic impacts as a result of low productivity, learning impairments and other impacts.

One University of Toronto study suggested the total economic loss due to iron deficiency was 4% of GDP, based on data from 10 developing countries.

NEED FOR DIAGNOSIS

The treatment, though, in most cases is straightforward and inexpensive – iron supplements. Experts say early diagnosis and monitoring can play the biggest role in tackling the disorder. That's where HemoCue, which specializes in point-of-care blood and urine testing, feels it can make a difference in India, where various public programs to combat anemia have shown slow progress.

> "The real-time data that HemoCue's system generates "can be instrumental for decision-makers to create policies around anemia management," HemoCue's Christ says.

The company, which has $20bn in annual revenue, has developed a system it calls *HemoCue HealthTrender Anemia* that it is now pitching to the Indian government. It can be used by health workers in urban and rural areas using *Bluetooth* connectivity and a mobile application.

The real-time data that HemoCue's system generates "can be instrumental for decision-makers to create policies around anemia management – we think it can be a game-changer," Christ said. "To diagnose anemia and make early crucial decisions related to managing anemia in patients and to monitor response to therapy, hemoglobin measurement remains the prime focus for treatment programs," he added.

The system uses a Bluetooth antenna to connect the *HemoCue Hb201* blood test and analyzer to a mobile app. A health worker then enters extra information into the app, such as gender, age, weight and height. That data is automatically transferred to the cloud and can be analyzed using a web service, which offers dashboards and statistical analysis.

The data can offer quick insight into the anemia problem at a school, in a community or at a wider level, and can help policy-makers target their programs. The tool also facilitates consistent monitoring of hemoglobin levels in groups that are being monitored. "We can get an instant snapshot of the situation, said Hema Divakar, a prominent Bangalore gynecologist, who was at the Nov. 30 launch.

DISEASE MANAGEMENT

Currently, blood test data must be manually collated, which, for a large sampling area, can take months and the process is error-prone. This means that anemia management policies are often based on either insufficient or unreliable data.

While making no commitment to adopt HemoCue's product, India's Ministry of Health deputy commissioner Ajay Khera said, "Right now, we're only reducing the anemia rate by 1% a year…here is a ray of hope that there is the technology available" to combat anemia "more effectively."

"While we're doing our best, we face formidable challenges, especially vis-a-vis quick and reliable diagnosis of anemia. Technology-based interventions can deliver fast results [and] data collation," Khera said.

Although anemia is a big problem in other developing countries, HemoCue's Christ explained that "in India the scale of the problem is beyond other markets; it's where we can see the biggest challenge." He said that targeting India first "really is a no-brainer [for us]; there's no other place in the world with [this magnitude of] problem."

He would not disclose the cost of installing HemoCue's system but said the price of the blood test per person was around INR40 (US$0.60), excluding cloud storage and analytics.

Published online 12/12/16

Cardiac Dimensions Launches IDE Trial of Carillon Mitral Repair System

REED MILLER reed.miller@informa.com

Cardiac Dimensions Inc.'s *Carillon* mitral contour system is moving closer to competing in the US mitral repair market with the start of the 400-patient CARILLON pivotal trial at about 50 sites, mostly in the US.

US FDA has approved an investigative device exemption for a trial that will randomize patients with symptomatic functional mitral valve regurgitation (FMR) associated with heart failure to either treatment with Carillon or medical therapy only, the company announced Dec. 1.

Both the patient and the trial's diagnostic core lab will be blinded to the treatment, Cardiac Dimensions CEO Gregory Casciaro said. The company expects the trial to begin enrollment in the first half of 2017. It will take about two-and-a-half to three years to complete enrollment, followed by at least a year of follow up for each trial subject.

The IDE trial is the fifth trial of Carillon. The company is also sponsoring the REDUCE FMR trial in Europe, Australia and New Zealand. The 180-patient trial, randomizing FMR patients to Carillon or medical therapy, is designed to secure reimbursement for Carillon outside the US. And published results from three trials in Europe support Carillon for the treatment of FMR. The 30-patient Carillon Mitral Annuloplasty Device European Union Study, completed in 2009, showed percutaneous reduction in FMR with Carillon is feasible, associated with a low rate of major adverse events, and improved the patients' quality of life and exercise tolerance. The TITAN trial in 2012 showed that Carillon implanted through the coronary sinus caused reverse left-ventricular remodeling with significant clinical improvements out to two years after implant. Results from 30 patients implanted with Carillon in the AMADEUS trial showed the device reduces mitral regurgitation and that permanent implant of Carillon can be achieved in most eligible patients.

Cardiac Dimensions' Carillon Mitral Contour Device

Photo credit: Cardiac Dimensions Pty. Ltd.

CLOSING THE SALOON DOORS

Cardiac Dimensions estimates that about 70% of the 26 million people with heart failure worldwide also suffer from FMR. FMR can overload the ventricle and accelerate heart failure, and many patients with FMR remain symptomatic despite medical therapy.

Casciaro explained that minimally invasive mitral valve repair with **Abbott Laboratories Inc.**'s *MitraClip* has become the dominant treatment for degenerative mitral regurgitation, which is caused by an anatomic abnormality of the mitral valve itself. But Carillon is intended to treat functional mitral regurgitation, which is usually caused by enlargement of the left ventricle. Abbott is also seeking the FMR indication for MitraClip with the COAPT trial.

Carillon is deployed through a venous route starting in the jugular vein. "It's very quick and comes through the coronary sinus, and it's just on top of the annulus of the mitral valve. We go in with a technology that is very quick to deliver. It's very easy to learn how to deliver this and it allows the physician to learn how to place it, and if they're not satisfied with the position they can remove it and reposition it during that sitting," Casciaro said.

He also pointed out that the Carillon implant procedure does not require much anesthesia – just a mild sedative – or anticoagulant therapy. Once the device is in place it reshapes the mitral annulus so the leaflets that have separated because of the disease will come back together again, he explained.

"The best analogy would be those old-fashioned saloon doors that almost touch each other – but don't quite – and swing open and shut. Visualize those being the leaflets and what happens over time is that door-jam that holds those leaflets has started to widen, due to age or whatever and the structure begins to break down," Casciaro explained. "What we do is fortify that doorway so those doors swing closer together and reduce the regurgitant process for the patient."

"It is pretty basic, and that's one of the beauties of it. It's an easy-to-learn, simply elegant approach to helping patients who are today underserved and very sick," Casciaro said. "For this challenging patient population, I think we're going to be a wonderful alternative, as has been demonstrated in Europe already."

Published online 12/9/16

CONTINUED FROM PAGE 6

does it communicate, what type of data does it communicate, how is the data secured, is there authentication, how difficult is it to break the authentication and so forth," he said.

He notes the recent stories about hackers being able to break into insulin pumps and pacemakers tend to use this approach. He also cautions it only took a few days and a few thousand dollars of lab equipment to achieve these objectives.

"We don't really want to compete on safety and security; we want to be collaborative with not only other members of the industry but also with their customers," says Steven Abrahamson, director of Product Security Engineering and Privacy at GE Healthcare.

Indeed, the growing number of reports of potential cybersecurity risks to medical devices has drawn the attention of not only industry insiders but lawmakers and the public in general.

HACKERS' TOOLKIT

To understand how a device communicates, hackers can use what are known as "sniffer" programs that sniff out any open ports on the device and what kind of data is being communicated via the ports. After discovering vulnerable ports, a hacker could try to access the data and/or the functioning of the device. If the data passing through the port is encrypted, a hacker could try to pick up packets of data being transmitted to the device to try decrypt the information and figure out how to manipulate the device.

"I'm not aware of any tools specific to medical devices, however [vulnerability testing tools] are readily available," said Wirth. "They're used by the bad guys for hacking exercises but also by the good guys to test equipment and evaluate equipment from the security perspective. Many of those are available for free."

One such tool is Metasploit, which is widely used by security researchers, or "white hat" hackers, to test equipment and devices, not just in health care but across all industries. However, the same tool is also used by malicious hackers, or what are known as "black hat" hackers.

"Once you map out the interface structure of your device, you then know very quickly which of those ports and interface protocols are exploitable because not all offer the same level of security," said Wirth. "And if you mix that type of knowledge in with past knowledge of, for example, the practices of device manufacturers to use default or even hackable passwords, many of which are widely published, then it becomes fairly easy to get into the devices and manipulate the device."

One of the simplest attacks is when hackers look for network weaknesses, such as by searching for unsecured network routers in hospitals that are visible to anyone and that are used to connect medical devices to the system. In this case, the burden falls on the network administrator, which typically are hospitals, to make sure their network is secure.

DEVICE-FIRM PROTECTION STRATEGIES

Michael McNeil, director of Global Product Security and Services Officer at **Philips Healthcare,** says his company takes into consideration the perimeter security controls available in the setting their device will be used. Philips factors in if the hospital has a firewall, such as an intrusion prevention system that inspects data communicating through a network, and that is able to block malicious traffic. The firm also checks to see if their device will connect to a network that uses intrusion detection systems that log and or alert users to any malicious traffic. That knowledge is applied to determine the security measures the they build into the products.

Another approach malicious hackers could use is to constantly flood a device with incorrect or negative inputs. That can sometimes overwhelm the device's processing capabilities.

"We typically don't test against negative inputs; we test against expected inputs," explained Steven Abrahamson, director of Product Security Engineering and Privacy at **GE Healthcare**. In order to try find such vulnerabilities, his company performs a type of vulnerability testing called fuzz testing.

However, he also emphasized, echoing other experts in the industry, that hackers typically have a monetary incentive to break into devices rather than wanting to harm or kill patients. As such, Abrahamson says it is important to figure out what the actual threat to patients and providers is. Malicious hackers are typically going to be interested in stealing patient data or crippling hospital systems to demand ransoms, he suggested.

According to some of the latest reports, malicious hackers seem to be changing their approaches from broader methods of attacking devices to more targeted attacks on patient data that can be sold on the black market.

While there are various methods hackers could use to break into devices, Philips' McNeil says hackers are likely to be looking for the "low-hanging fruit" if they try breaking into a device, such as using the online Shodan search engine that can be used to find devices connected to the internet.

"Using standard types of scanners, sniffers that are easily available for exploits, that's the easiest way to get into devices," he said.

But it's not just that tools are easily available to hackers with malevolent or benevolent intentions, says Wirth. He notes there are complete hacking services out there for people who have no technical skills in the area.

"We live in a day and age where the hacker-for-hire economy out there has really changed the cyber landscape," he said. "In this day and age, you can buy any service, any type of data, and any type of tools out there."

Codenomicon is one such company, which was bought by Synopsys in 2015, that provides fuzz testing tools. Such tools can be very effective at testing device interfaces, but there are also a lot of similar products on the black market that can be used for "more shady purposes," according to Wirth.

COMPANIES COME AROUND TO 'WHITE HAT' HACKING

One problematic area for security researchers trying to do a public service by testing medical devices for vulnerabilities is they risk violating the Digital Millennium Copyrights Act. Under the law, software is typically protected as intellectual property and therefore reverse-analyzing it to try to understand it and figure out how the protocols work could be treated as copyright infringement. However, Wirth says there are efforts under way to change the law to try exempt security researchers from prosecution.

"The logic put forward, I'm not saying that I necessarily share it – I'm somewhat ambivalent about it – but basically the logic is that security researchers perform a service to the public by helping manufacturers identify device vulnerabilities and therefore they should be legally protected," he said. "There have been other cases where there have been other lawsuits brought against security researchers not only in the health-care medical device space."

However, in recent years Wirth says device companies have come to realize the researchers are assets to their business. As an example, most recently, Johnson & Johnson announced it was working with Jay Radcliffe, a senior security consultant and researcher at Rapid7, who discovered a security loophole on their *OneTouch Ping* insulin pump to mitigate the problem. The hacker's and company's partnership is exactly the kind of collaborative approach US FDA has been urging industry to use.

"We see that, more and more, companies are now opening up even to the point that they're offering bug bounties and they're opening up to security researchers reporting to them and engaging in an open dialogue, because the assumption is that open dialogue in the long run is more beneficial than to pretend everything is OK, and fight back somebody that comes to you and reports a problem or vulnerability," Wirth said.

In just the past few years, several major medical device companies have not only engaged with security researchers but have developed their own internal cybersecurity labs and teams to test their devices in controlled settings.

GE's Abrahamson says his company has a team of 30 cybersecurity experts spread out mostly in the US and, Europe, with a few in Bangalore, India. They are a mix of white hat hackers and experts in risk assessment who bring together the technical expertise to understand how a device could be broken into, and also what kind of threats particular vulnerabilities actually pose.

"Sometimes you have to think like the bad guys to protect from the bad guys," he said.

Abrahamson says the first step his team at GE takes is to ask what are the different types of risks the firm's devices may face. Sometimes that risk is based on whether hackers would have any incentive to change the intended use of the device and, in so doing so, figure out what kinds of unintended use they could make the device perform.

They also try to determine if a hacker may have any motivation to steal the data that is either stored on the device or that is communicated to the device, and what the hacker would have to do to obtain patient data or unauthorized access.

A more sinister risk, and one that has been dramatized by Hollywood but is far less likely, is hacking into the device to harm a patient. Such scenarios typically don't come with a monetary benefit to potential hackers.

So, far Abrahamson says one of the biggest, real-world concerns within industry are hackers using medical devices to insert ransomware into health-care system networks. Using this approach, a malicious hacker could block health-care providers from accessing patient data and demand a ransom to have that data unlocked.

Cybersecurity experts have been stepping up efforts to warn industry and FDA about the dangers of ransomware this year, especially as several high-profile attacks targeting major hospitals around the country have in many instances temporarily crippled the facilities' ability to treat patients. So far there have been no reported cases of patients being harmed from such attacks, but it's also of high interest because of the potential financial losses that could be result.

McNeil says he uses a combination of internal and external cybersecurity experts to help him test devices at Philips. Internally, he has product security officers that are individually responsible for assessing the risks of a specific type of product within the company's pipeline. On top of that, he employs white hat hackers, who come in later in the product development process to try break into a device to make sure the security on the product is strong.

"I have a dedicated team who are certified security professionals; they are truly passionate about hacking devices and they are assigned different devices based upon our release schedules and they are responsible for hacking these devices," he said.

The team is assigned different use-cases to imitate realistic settings. Sometimes due to constraints on time and resources, McNeil hires third-party organizations to run the tests.

"In some cases, I may just use an external [organization] because I want to use them as a validation or verification of processes that we have in place," he added.

MEDTECH'S SHIFT TO CYBERSECURITY WORKFORCE

Abrahamson explains that it was about a decade ago that GE became more concerned about improving cybersecurity on the company's devices. At the time, several of its engineers started thinking of ways to protect the products from potential attacks. About six and a half years ago, the company decided to roll out a formal program, as part of its design process, to develop better cybersecurity features. However, GE soon realized that many of its engineers didn't have expertise in cybersecurity. That's when the firm began hiring experts from tech companies that weren't, until then, involved in the medical device industry.

"We had to, first of all, bring in a few people with adversary mentality, but also the security expertise in the medical community didn't exist to the level we needed it," Abrahamson said. "So we brought in people from other industries with more maturity and supplemented that with program management and experts with more medical device expertise."

GE hired people from companies such as Microsoft who could help them better understand how their devices may interact with *Windows* operating systems used in hospitals; experts from Motorola who could help develop better wireless communication protocols; and people from the health IT sector who could help assure compliance with patient privacy and safety.

Abrahamson says the company has also had to do a lot of internal development, implementing training courses to help staff without cybersecurity expertise get up-to-speed.

But it remains a good market for cybersecurity experts in the medtech sector. Device companies say there is a shortage of experts available to help them design and maintain security for their products; some say cybersecurity experts who want to work in the device industry are virtually guaranteed a job.

According to a report by Cybersecurity Ventures, the unemployment rate in the field was zero percent in the third quarter of 2016. Abrahamson affirms that while there are a lot more cybersecurity experts in the medical industry today, with many of them having been trained internally, it is still an acute issue for industry to find people with the right blend of cybersecurity and medical device expertise. He says he's heard the unemployment rate for cybersecurity across industries could be as low as minus 14%. To get over that problem, GE has been not only bringing in outside experts but marrying them up with internal experts and emphasizing training efforts.

"We have internal training we have developed and we use our internal experts to train our engineering teams on health-care specific security processes, and then we also use general secure development industry-level training that is more broadly applicable and we train a broader segment of our development community," said Abrahamson.

More recently, CDRH Director Jeff Shuren has even encouraged medical device companies to hire hackers to help build defenses.

In 2013, when GE rolled out its internal design engineering process called Design, Engineering, Privacy and Security (DEPS), it used a three-step risk-assessment process to identify appropriate security controls, privacy risks and security failure modes. As part of the process, Abrahamson says the company has trained at least 800 medical device engineers and employees from other GE sectors using two- to three-day-long boot camps, as well as a compressed three-hour Web presentation. The company also uses a mostly computer-based training course and curriculum that it assigned to several thousand of its development engineers a few years ago; it is gearing up for another round soon.

Philip's McNeil says certain academic institutions such as Boston University and Northeastern University are also developing curricula to funnel their students trained in cybersecurity into the medical device industry.

"Yes, there is a potential shortage, but the way that we at Philips have tried to combat that issue is to have a set of dedicated resources and a dedicated team. I'm in a much higher ability to attract and retain people from an organization perspective than if it was something that was done on an ad-hoc basis," he added.

On top of that, McNeil says his company is able to participate in training with external cybersecurity experts, especially from academic organizations. Often they also hire experts from academia as interns and, in other instances, the firm sends people from Philips back to academia to get more training.

TIPS FOR SMALL FIRMS

However, not all device manufacturers are alike. Large companies like GE and Philips have the resources to draw cybersecurity experts and conduct device testing to a degree likely lacking at most smaller companies. To level the playing field somewhat, Abrahamson says smaller companies need to get involved with cybersecurity collaborative organizations that give them a chance to communicate and share concerns about cybersecurity.

"We don't really want to compete on safety and security; we want to be collaborative with not only other members of the industry but also with their customers," he said. "I spend a lot of time meeting with and working with customers on what we can build into our processes and how we can better support what they're trying to do."

A key organization Abrahamson recommends smaller companies join is the Medical Device Innovation, Safety and Security Consortium (MDISS), which has been an active advocate for developing testing standards and recommending requirements to keep devices safe.

Abrahamson says cybersecurity conferences are also a great resource. He also says industry is lucky that FDA has been so open to developing collaboration between industry, security researchers and patient groups to address concerns with medical device cybersecurity.

"We actually are able to work with FDA in some of those industry groups particularly through MDISS where we can help arrive at guidance for industry that makes sense," he added.

McNeil says regardless of how small a company may be, it needs to understand the importance of investing in people who understand cybersecurity well enough to at least ask the right questions. The big question they need to be able to ask is how each device is going to function in its intended environment.

"As they're working with other vendors and as they're procuring solutions they sort of have an opportunity to raise the bar," he added.

McNeil says from a regulatory standpoint, companies need to conduct some form of testing and, even if they don't have the resources to conduct internal testing, there are organizations out there that can do the testing for them.

"I do know of other organizations that are looking at recommendations around having centralized testing capabilities that some of the smaller regional entities are trying to develop their

solutions [around]," McNeil added. "If smaller organizations have access to pooled resources from other entities, then that can also …get some appropriate testing done before their solutions are brought to market."

He says there are various entities that are currently piloting such solutions, but they are early in their development so he declined to provide details.

MOVE TO TRANSPARENCY?

Moving forward, Abrahamson says the key to better security is transparency. Over the years, GE has been monitoring its devices for potential vulnerabilities that are identified by the industry, he said, to determine if the company needs to take any action and if so, what action.

GE has tens of thousands of devices in the field, including products that the company services. Abrahamson says they screen those service activities to look for any potential security incidents.

"When people talk about what's the risk, we have a pretty good idea because we are screening tens of thousands of service calls on a monthly basis," said Abrahamson. "I would say we have a long way to go there, but we have a good foundation in place and there's a lot of industry activity going on, on how we effectively share information on vulnerabilities."

There is an ongoing debate in the industry on whether companies should guard their software so people aren't readily able to understand the code. Proponents of using proprietary software argue it makes it much harder for hackers to break in and figure out how to manipulate products.

On the other side, some argue that open-source software is the way to go so the software language is available to anyone to read and understand. That, they argue, gives a lot more people the chance to figure out if there are any security flaws in the code that needs to be fixed.

GE's products use a mix of off-the-shelf software, such as Windows and *Linux* operating systems, and proprietary software. Abrahamson says his view is that the device industry is heading more toward open-source software. But he says that will take time because customer IT organizations often still prefer to use operating systems like Windows due to familiarity.

Wirth says that, besides device manufacturers, there are also some large hospitals, such as the Mayo Clinic in Minnesota, who have started doing their own device testing and publishing their findings.

"The problem with hospitals doing it is obviously that after you're done with the testing, you need to rebuild the device so that you need to make sure you have not inadvertently changed anything inside the device which could affect the safety of the device," he said. "Therefore, I think this type of exercise is probably limited to hospitals that have more devices available, and also have more money that they can spend on projects like this."

Wirth says that device testing labs such as Underwriters Laboratories (UL) are also conducting similar security assessments that include certifying security on devices to certain standards. There are also a growing number of academic research organizations such as the Archimedes Lab at the University of Michigan and the Independent Security Researchers (ISE) at Johns Hopkins University that have become important resources for cybersecurity research.

According to Wirth, it's a good sign that in the past few years more and more stakeholders from different sectors are starting to team up and work collaboratively to solve problems. In the past, device companies and security researchers had a more antagonistic relationship that was a hindrance to improving products. Now, he says, the collaborative model has led to companies actively working with researchers who discover potential risks to find ways to tackle vulnerabilities.

"A couple of years ago it was more individual researchers buying a medical device on eBay, hacking the hell out of it and then in several cases what happened was they went to the medical device manufacturer, they wanted to report what they had found, they got pushback, nobody wanted to talk with them, the manufacturer wanted them to go away, and then they went to the FDA, Homeland Security and the press," he said. "Then we have those big stories over the last couple of years. I hope we are out of that, I hope we are at a more meaningful stage, in the sense that now we see the more systematic evaluation, we see now the manufacturers doing their own testing and I think we see more open and constructive communication between stakeholders on the topic."

Wirth says the medical device industry is moving away from an "uncontrolled state" with cybersecurity to a state that is based more on constructive cooperation between stakeholders, which ultimately better serves everyone, especially patients, he argued.

"One concern I have about the current discussion is that in many cases we see too many initiatives pop up and too many people trying to do the same thing with maybe conflicting results," he added. "I always say jokingly that I wish somebody would step up and coordinate the willing, but at the same time it's a huge step forward to where we were like one or two years ago."

CLICK

For details on the evolving regulatory landscape efforts in cybersecurity go online at http://bit.ly/2gHNdBO.

Published online 12/9/16

CONTINUED FROM PAGE 5

factured SUDs. Going forward, adopting the UK's approach to nomenclature and consistent with the manufacturer paradigm for SUD reprocessing to be adopted as part of this MDR, AMDR's members will use the term "remanufacture." "Reprocessing" is typically understood to take place in hospitals; we have chosen to use the term "remanufacture" as our members remake devices meeting all manufacturer standards.

What are the implications for remanufacturers, notified bodies, the competent authorities and the European Commission of the new rules?

Vukelich: Firstly, patients and health-care providers now have assurance that reprocessed or remanufactured SUDs meet the same safety requirements as any other CE-marked device.

Secondly, original equipment manufacturers have long lobbied for strict requirements for SUD reprocessing. The MDR now "levels the playing field" in that entities that want to reprocess SUDs must meet the same standards as any other manufacturer. Frankly, as SUD remanufacturers now need to meet all the same MDR requirements as any other manufacturer and await member states to affirmatively opt in, the standard for SUD remanufacturing is now higher than it is for most manufacturers. From our perspective, this un-levels the playing field.

Thirdly, the situation is far more complex for competent authorities and notified bodies.

Competent authorities now must assess the final regulation and decide if they want to allow CE-marked remanufactured SUDs on their market. This is something we hope and are urging authorities to do as CE-marked remanufactured devices will meet the same standards as all other devices, but offer lower-cost and environmentally preferable options for hospitals – desperately needed in an era of limited health-care resources.

Notified bodies must also decide if they want to work with SUD remanufacturers. With the limited number of notified bodies growing even smaller, and the requirements growing more intense, AMDR members are concerned at the lack of available notified body options. This will have the effect of increased costs for remanufacturers, increased time to access the market, which leads to increased costs and reduced availability of remanufactured devices for health-care providers.

How soon do you anticipate that the structures will be in place to enable remanufacturers and notified bodies to meet these rules?

Vukelich: This is an unknown. AMDR members are working tirelessly now to obtain CE marks and preparing to meet the new MDR requirements. Having member states' competent authorities opt in and greater notified body participation with remanufacturers will speed things up.

When will remanufacturers need to comply with these rules?

Vukelich: AMDR understands the MDR's requirements for SUD reprocessors will come into effect according to the same timeline as all other requirements. Existing MDD requirements already provide the pathway for us to obtain CE markings for our current reprocessed products.

EU policymakers ran into challenges in reaching agreement on the forthcoming rules for reprocessing. Can you explain briefly why this was and whether the agreement that has been reached is the most workable solution in your view? And if not, why not?

Vukelich: This is an excellent question. Fundamentally, we believe the reprocessing provisions were unnecessarily contentious because not everyone at the negotiating table was talking about the same thing.

Many hesitant to accept that SUDs could be reprocessed were doing so based on their experience and understanding of hospital reprocessing of reusable devices. Reprocessing in hospitals is not the same as reprocessing of SUDs conducted by regulated, commercial firms. It was not fair to compare the two. In fact, the European Commission's original report on SUD reprocessing only looked at in-hospital reuse and it was unfair to make conclusions about regulated commercial firms based on what was taking place in hospitals – it is comparing apples to oranges.

MDR Provision

The MDR (Recital 31) outlines the way forward for single-use device (SUD) reprocessing. It states:

"The reprocessing and further use of SUDs may only take place where permitted by national law, and in respect of the requirements laid down in this regulation.

"By reprocessing a single-use device with the view to make it suitable for further use within the Union the reprocessor should be considered the manufacturer of the reprocessed device. By way of derogation, Member States may decide that the reprocessing and re-use of SUDs within a health institution may vary from the obligations of the manufacturer described in this Regulation. In principle this is only permitted when adequate common specifications are in place and if appropriate national regulations exist and are applied in the reprocessing of these devices which ensure at least the same level of security as in case of the corresponding initial SUDs. This also applies if the reprocessing is carried out by an external reprocessor on behalf of a health institution."

Furthermore, the reprocessing terms that have been agreed within the context of the Medical Devices Regulation are not the most workable because they are not harmonized – because member states can choose not to opt in – and the forthcoming in-hospital common specifications has become a major distraction, in our opinion. [**Editors' note:** *The current Article 15.1c* instructs the European Commission to develop the common specifications for in-hospital SUD reprocessing by the date of application of the regulation.*]

In AMDR's view, in-hospital reprocessing of SUDs will soon be a thing of the past, which it should be, in our opinion. The continued focus and hope that some member states have expressed that their hospitals can continue to reprocess in-house and meet new forthcoming standards is unfounded, we think.

What will be involved for the European Commission in keeping the list updated?

Vukelich: Lists of devices that can or cannot be reprocessed were contemplated in earlier versions of the regulation but ultimately NOT included in the final regulation. This is a moot point. If a remanufacturer cannot meet the MDR requirements, the device will not be entitled to display the CE marking and will not be marketable. If a remanufacturer does demonstrate to a notified body it has met the requirements, it is entitled to display the CE marking.

How much transparency will there be when it comes to remanufacturing?

Vukelich: There will be full transparency. Like for any other medical device manufacturer, SUD remanufacturers will mark and label the devices with our names and logos and will comply with UDI requirements. We will comply with adverse event or vigilance requirements and we will only engage with hospitals that contract with us to provide our devices. We are responsible companies and we stand behind our products.

Why may there be different rules in the future around Europe? What about possible hospital exemptions?

Vukelich: In our view, the Article 15* in-house reprocessing provisions will ultimately have little impact. At a minimum, the MDR requires that hospitals wanting to reuse SUDs in-house must have a risk management program in place, which includes the "analysis of the construction and material, and related properties (reverse engineering)" of the device, have a quality management system, have validated all procedures and conduct product release and performance testing, to name a few examples, plus meet forthcoming "common specifications" to be released by the commission; and compliance with all the common specifications shall be certified by a notified body. AMDR does not believe hospitals are able to meet this standard. Even if they are, we are unaware of any notified bodies willing to undertake such a certification. Thus, while we have yet to see what the common specifications will be, we believe this high standard will ultimately steer hospitals to commercial, regulated, CE-marked remanufactured SUDs, rather than use in-house.

What are the biggest risks in remanufacturing in the future, in your view and how will it be policed?

Vukelich: Remanufacturers, like any other device manufacturer, are subject to all the same enforcement rules, plus member states must affirmatively opt in to allow such products on their market. As to hospital reprocessing, many member states have expressed concern that they lack the resources to effectively ensure hospitals are not reprocessing SUDs in violation of the rules of the MDR.

To that, AMDR encourages member states' Ministries of Health or competent authorities to issue letters or clarifications to all health-care providers that new, forthcoming EU rules place stringent manufacturer requirements on the reprocessing of SUDs and therefore, any entity reprocessing SUDs and not demonstrating conformance to the requirements is subject to enforcement action. This would also be an opportunity for the member states to alert hospitals that the member state has opted in, giving hospitals access to lower-cost, environmentally preferable CE-marked remanufactured SUDs.

What will the liability scenario look like?

Vukelich: The SUD remanufacturer assumes regulatory and legal responsibility for the devices they make – just like any other manufacturer. SUD remanufacturing has been regulated as manufacturing in the US by FDA since 2000 and in Germany since 2002. In both regulatory frameworks, the name of the SUD remanufacturer is placed on the label and packaging as the responsible manufacturer, just like any other manufacturer. And adverse event reporting/vigilance rules apply just the same – just like any other manufacturer. AMDR is not aware of any instances in which the original equipment manufacturer has been held legally responsibility for the inadequate reprocessing or remanufacturing operations of a third-party.

***[Editors' note:** *The article numbers in the MDR are subject to change when the final version of the regulation is issued. Reprocessing requirements reside in Article 15 of the latest version of the forthcoming MDR, but they may end up in Article 17 in the final text.*]

Published online 12/7/16

Possible Trump FDA Commish Candidate Favors (Much) Lighter Touch

FERDOUS AL-FARUQUE danny.al-faruque@informa.com

A purported candidate to run FDA under the Trump administration would bring what some consider troubling views and experience to the commissioner post, but regulatory affairs stakeholders say Silicon Valley investor Jim O'Neill could be an interesting pick.

According to information first reported by Bloomberg, President-elect Donald Trump is considering replacing FDA Commissioner Robert Califf with O'Neill, an associate of the controversial Silicon Valley billionaire investor Peter Theil who backed Trump during his presidential bid.

Previous public statements by O'Neill suggest he favors a much reduced role for FDA. He has advocated reforming FDA so that products could go to market solely based on their safety profile and not require evidence of efficacy. In a 2014 speech, he said it should be up to patients to take the risks associated with an unproven drug and efficacy should be proven after product has been legalized.

The Trump transition team has not confirmed the report that O'Neill is under consideration. Another potential candidate whose name has been floated for the FDA commissioner post is Scott Gottlieb, a physician, American Enterprise Institute resident fellow, and former FDA and CMS official who recently joined Trump's transition team.

Significantly, O'Neill is not a physician, typically considered a key qualification for an FDA chief. But he does have government experience. He began working at the US Department of Health and Human Services in December 2002, during the administration of George W. Bush, as a speechwriter to the secretary on topics including the Medicare Modernization Act, Medicaid Reform, drug approvals and health information technology. In August 2005, he took on the role as an associate deputy secretary at HHS and served as a senior advisor to the deputy secretary.

Finally, in November 2007, he became principal associate deputy secretary where he advised the HHS deputy secretary on various issues including on FDA topics.

> "Nobody can just become FDA commissioner and change the system wholesale. There will be a lot of discussion. Ultimately, Congress has to approve," attorney Jeffrey Shapiro says.

After his stint working for the government, O'Neill moved to the private sector to work as managing director for Clarium Capital Management in San Francisco, and eventually joined Thiel's tech investment firm Mithril Capital Management as managing director, where he's been for almost five years.

A source with extensive knowledge of FDA operations told *Medtech Insight* that O'Neill may be a problematic pick for commissioner because, while he is a visionary, he lacks the management experience that most commissioners tend to bring with them to the job.

"I think that he's clearly not in the traditional profile [and] some people feel committed to the traditional profile," the source said, on condition of anonymity because he works closely with the agency. "Whatever job he wants he's got it, but FDA commissioner may not be the right job for him. But it's also not a given he'll be at FDA."

O'Neill's comments about FDA's role align with the views of his boss, Thiel, who is a staunch and outspoken Libertarian. O'Neill is associated with The Seasteading Institute, cofounded by Thiel, which advocates establishing "floating cities" that can operate without conventional government intervention.

In the medtech space, O'Neill has said he opposed FDA's regulation of companies such as 23andMe Inc., which got pushback from the agency a few years ago for claiming to be able to provide health information based on consumer-directed genetic testing that had not been vetting by FDA. 23andMe ultimately worked through its challenges with FDA, bridging what has sometimes been complicated communications gap between Silicon Valley firms and the agency.

FRESH THINKING?

Jeffrey Shapiro, an attorney with Hyman, Phelps & McNamara who represents companies on FDA matters, says O'Neill could be an interesting pick because of his business background, rather than having a standard medical background.

"The idea of bringing in a business person rather than a doctor is interesting because certainly in the device arena, device investors say some of the regulatory approaches to device pre-market review is discouraging investment," he said. "Someone like that may have ideas on how to foster more innovation."

Shapiro says O'Neill could bring fresh thinking to the agency and an outsider

CONTINUED ON PAGE 22

CONTINUED FROM PAGE 1

stringent Level 2 inspections, during which investigators review all four subsystems.

FDA emphasizes that only select elements of QSIT are used during rigorous compliance follow-up, for-cause and risk-based inspections – but those types of inspections are outliers.

"Quality system inspections should generally be conducted using the Quality System Inspection Technique, and each inspection report is reviewed by regulatory officials in the agency for quality control. The FDA also performs audits of the program to help ensure that proper procedures are followed," the agency noted in its Nov. 22 email.

"bottom up" method to auditing. But QSIT emphasizes a "top-down" approach; that is, an investigator will look at a firm's systems for addressing quality first before reviewing any specific quality problems.

"You could just tell by that investigator's words, his questions, his language – everything – that he wasn't comfortable using QSIT. When he got into design controls, he was uncomfortable. He didn't feel confident in management controls. He was not comfortable at all."

QSIT was a collaboration between FDA's Center for Devices and Radiological Health and the Office of Regulatory Affairs, which handles all of the agency's field activities.

The predictability of QSIT allows firms to prepare for an audit appropriately. Investigator deviations from the technique mean less predictable audits and, quite possibly, unfavorable inspection outcomes for the companies.

FDA offers the QSIT guide online and routinely instructs manufacturers to download the document so they'll know exactly what an investigator will look for during an inspection. The predictability of QSIT allows firms to prepare for an audit appropriately. Investigator deviations from the technique mean less predictable audits and, quite possibly, unfavorable inspection outcomes for the companies.

Wells conceded that FDA likely isn't instructing investigators to bypass QSIT during Level 1 or 2 inspections; rather, the problem lies with select investigators who choose to audit their own way.

"For example, I attended a foreign inspection; I was in the front room where the investigator works. The investigator had the QSIT manual in front of him. He had it on the table. He asked a couple of questions, but then you could just tell that his comfort zone was complaints, and he was in his element," said Wells, who is currently president of consulting firm QualityHub.

Beginning an inspection by looking at a firm's complaints is considered to be a

The technique is merely the third and bottom layer of FDA's activities around facility inspections. QSIT is used in conjunction with the Investigations Operations Manual which, in turn, is used with the Compliance Program Guidance Manual.

The IOM is the primary source regarding FDA policy and procedures for investigators. Meanwhile, the CPGM directs investigators on how to conduct an inspection for a wide variety of products, including medical devices, drugs, biologics and vet medicine. FDA has been using a device-related compliance program since the 1960s and revises it every now and again. It was last revised in February 2011.

The CPGM "outlines the inspectional strategy and provides guidance for inspectional coverage." It points out that "flexibility" is feasible when conducting inspections, FDA noted in its email.

But Wells says some investigators routinely take advantage of such flexibility by slipping into a comfort zone.

"I can see why FDA would have investigators that don't necessarily follow QSIT to the letter. That's because they're going to look at stuff they're comfortable with," Wells said. "For example, investigators with an engineering background love design controls and production controls. They are bored by CAPA and complaints, and even gloss over them. But there are other investigators that love CAPA and complaints, and won't hardly touch design controls.

"QSIT served a purpose at a time in history when there needed to be guidance around inspecting to FDA's Quality System Regulation, which included new items such as design control and management control," he continued. "Part of it was teaching investigators that there was a new regulation, and QSIT helped investigators ask the proper questions."

But the Quality System Regulation, released in 1996, "is not new anymore," Wells said, which has the effect of pushing some investigators their own way.

"What's happening is that investigators are gravitating to their comfort zones," he said. "A lot of the investigators aren't held accountable in terms of their style or their mannerisms of doing inspections. We knew right after QSIT was launched that certain investigators wouldn't follow it. But there's no policing that I'm aware of where FDA says, 'Hey, you didn't follow QSIT. You forgot to do that. How come you didn't ask them that?'"

Pam Weagraff of consulting firm Quintiles IMS pointed out that it isn't out of the ordinary – or necessarily wrong – for investigators to gravitate toward comfort zones.

"If an investigator has expertise, say, in cleanrooms, and he or she is looking at production or process controls, then they may delve a little deeper into cleanrooms because that's their area of expertise," Weagraff told *Medtech Insight* on Dec. 5. "Or, let's say an FDA investigator has expertise in software, so by going through design control, he or she might dig deeper into software development practices. So historically, that's not unusual."

Weagraff is director of Quintiles' Medical Device and Diagnostics Regulatory Group, within the firm's Regulatory Quality and Compliance Group.

Between 1999 and 2003, Weagraff worked with device trade industry group

AdvaMed and the Health Industry Manufacturers Association to write three "points to consider" guides to help manufacturers better understand FDA's QSIT approach to corrective and preventive action, design controls and management controls, comprising 65 pages of material.

OTHERS SEE DIVERGENCE FROM TECHNIQUE – INCLUDING SECOND QSIT AUTHOR

There are others in industry who agree with Wells' assessments, including Jon Mullen, VP of quality for device-maker Cynosure, who says some investigators simply don't stick to QSIT when inspecting.

"I wouldn't disagree with that statement, that investigators aren't always following QSIT," Mullen said in a Dec. 5 interview with *Medtech Insight*. "Not that they're going rogue inspecting things they shouldn't be, but it does seem like many investigators have their own processes – processes that aren't necessarily based on the steps of QSIT."

Cynosure is a maker of light-based aesthetic and medical treatment systems, such as *Accolade* for removing lesions and *Cellulaze* for eliminating cellulite.

At a device firm where Mullen previously worked, the investigator didn't review CAPA during the QSIT inspection. "That didn't make sense because CAPA is the heart of your quality system. Basically, all of your problems go in your CAPA system, so it's a very valuable tool for an investigator to figure out where your soft spots are," he said. "And because CAPA is at the heart of QSIT, a QSIT inspection without a CAPA review is, by definition, not a QSIT inspection."

Mullen kept his mouth shut when the investigator failed to look at CAPA during the QSIT audit. "I would not offer up, 'Investigator, hey, let's go through my CAPA system. You didn't ask about it.' It's crazy for them not to go there because if you have a defective CAPA system, you're absolutely going to find where the problems with the company are. When you're sitting in an FDA inspection, there's one thing you want, and that is for the inspection to be over. While an investigator is there, there's danger – danger that things are going to come up."

Aside from Tim Wells, six other device center and ORA officials – and three advisors – made up the rest of the core QSIT team when the document was drafted in the late '90s. Among them was Denise Dion, an 18-year veteran of FDA where she served as an investigator. Dion, who helped write QSIT as part of ORA, is currently VP of regulatory and quality services for consulting firm EduQuest in Hyattstown, Md. She spoke with *Medtech Insight* on Sept. 27.

Dion was adamant that she, too, sees FDA investigators simply not following QSIT and she says it's a common occurrence. (See box, "Denise Dion's Take.")

"I've been in the front room for inspections and I know they're not following QSIT," she said. "And I've been in the back room, seeing the many different items that the investigator asks for. I notice that they are items that typically aren't asked for during a QSIT inspection."

Dion pointed to the Compliance Program Guidance Manual. Under Part III, Sec. A1a, the guide states that quality system "inspections should *generally* be conducted using the Quality System Inspection Technique." (Emphasis added.)

"Well, *generally* investigators are going to follow QSIT, but that doesn't mean they *have to* follow QSIT," Dion said.

But that's nonsense, says a former director of FDA's Investigations Branch. Ricki Chase, now compliance practice director at Lachman Consultant Services Inc., left the agency in June.

"What if the [CPGM] said, 'You *will* follow QSIT'? Well, if you *will* follow QSIT, that means that during an abbreviated inspection the investigator *will* do X and *will* do Y, and *will not* do anything else because they *will* follow QSIT," Chase said in a Nov. 8 interview.

"So then what? Should the investigator ignore public health risks because he or she *must* follow QSIT? That doesn't make any sense," she added.

In her role at FDA, Chase was responsible for all operations of the Investigations Branch, including inspections, investigations, sample collections, consumer complaints, import operations and emergency-response programs.

Denise Dion's Take

Medtech Insight: How do you know that investigators are not following QSIT? Are you basing this on inspections of your customers, your clients?

Denise Dion: I've been in the front room for inspections and I know they're not following QSIT. And I've been in the back room, seeing the many different items that the investigator asks for. I notice that they are items that typically aren't asked for during a QSIT inspection.

MTI: Does this happen during a lot of inspections?

Dion: Yes.

MTI: I want to make sure that you feel comfortable saying that. That's a strong statement to make, I assume, that many investigators aren't using QSIT. I just want to make sure that you feel like you've seen enough inspections that you believe there might be a trend of investigators not using QSIT. Am I correct?

Dion: Yes.

"The investigator should have the skillset to make a decision about which complaints they're going to look at or which processes they're going to look at. That is supposed to be their professional judgement in the moment, on the job. They're the one doing the audit – not somebody sitting at a desk somewhere who's not there with their hands in the mess," Chase said.

"You have to allow the investigator the ability, based on their training and their knowledge, their skillset and their experience, to make judgement calls," and sometimes drift from QSIT.

QSIT, Chase says, often begs the question: "Why do medical device investigators need somebody to tell them how to specifically conduct an inspection?"

"Well, quite frankly, I don't think that they do need it," she said. "If you train your people on what the regulation is and they have good technical skills, and they understand FD&C law and they can make good, sound judgements based on fact, which they can document in a report – why do you need anybody to tell you to follow an inspection technique? And why can't you allow them the discretion to make good decisions in the course of their duties? That's the real question."

Chase says "no one should make generalized statements that all investigators don't follow QSIT."

Of course, there are "individuals who willfully do not do what they're trained to do or what they're supposed to do – sure, those types are at FDA, but they're not abundant. They just simply are not abundant," she said.

But, indeed, "there are some investigators that don't follow QSIT because they don't know what in the world they're doing. There are some investigators that aren't following QSIT because they think they can do their own darn thing. And then there are some people out there who aren't following QSIT for a given reason – it's probably because there are other factors or extenuating circumstances which would be explained in the [Establishment Inspection Report] as to why they did what they did."

Chase pointed out that when investigators' work is reviewed by supervisors, it will be checked to make sure that QSIT was used as a roadmap.

Nevertheless, "If an FDA investigator is assigned to a Level 1 inspection, they should be staying on point and doing a Level 1 inspection, which means they should be doing CAPA plus either design controls, or production and process controls. And that's what they should focus on," she said.

"They shouldn't expand beyond that without some very good reason," Chase added. "Sometimes you see people who just can't help themselves, and they can't seem to stay on point and they start wandering off. And that's usually a sign of immaturity more than anything. Not a sign of willful intent."

Still, she said, having an investigator at your facility that helps find problems by slightly veering off the QSIT path isn't necessarily a bad thing.

"The question is, do you want the investigator who follows QSIT and looks at, say, only 11 complaints, fills out the FDA-483 form and walks away because that's what they're supposed to do?" Chase said. "Or do you want the investigator to says, 'Well, I know that's what QSIT says I'm supposed to do, but I also know that based on my experience I think they have a much bigger problem than just these 11 complaints.' I'd like to think that manufacturers would like to know about the problems."

"But does it happen? Yeah, it happens. There are rogue investigators out there. I've worked with them. I've managed them. I've directed them. They exist."

In general, investigators that most closely follow QSIT are those who are new to the agency.

"The new investigators are so terrified that they're going to make a mistake that they tend to be very slow and very methodical, and very by-the-book," Chase said. "They follow the QSIT manual line-by-line-by-line because they don't want to make a mistake. So, your newer investigators – while they may be less experienced on the technological side – they're very, very by-the-book."

"There are some investigators that don't follow QSIT because they don't know what in the world they're doing. There are some investigators that aren't following QSIT because they think they can do their own darn thing," former FDAer Ricki Chase says.

FRESH INVESTIGATORS FOLLOW QSIT TO A 'T'

Perhaps surprisingly, veteran investigators are more likely to deviate from QSIT during an inspection, former FDAer Chase said.

"What I tended to find during my time at FDA was that when you have senior investigators, particularly people holding the title of 'specialist' or 'expert,' they think the rules don't apply to them. And they tend to just wander all over the map, and they say all kinds of things they shouldn't say. And they do all kinds of things that they shouldn't do. It pisses people off, and rightly so. And it happens. And when it happens, and the district management is made aware of it, the individual is counseled.

"If they have to be continuously counseled, then it becomes not only a performance issue, but also a conduct issue. And there are steps in place to address that," Chase continued. "I won't comment on whether I think those steps are effective, but there are steps in place that are intended to address those types of behaviors.

DO FIRMS EVEN COMPREHEND QSIT?

Sure, an industry quality-systems expert would likely notice if QSIT was not followed by an FDA investigator. But would a run-of-the-mill staffer at a device company even know if an auditor strayed from QSIT? Chase said she isn't sure.

"There are a lot of manufacturers that don't know how to follow QSIT – in fact, there are a lot of them out there that don't," she said. "And they don't know what QSIT really means, and they don't know how investigators are trained to interpret what QSIT means."

After all, "there are plenty of manufacturers out there that don't even have an SOP for how to handle an audit or how to handle an inspection. There are a lot of manufacturers out there that don't do mock audits," Chase said.

"Are those companies familiar with QSIT? Yeah, they probably read it. Just like they're familiar with the [Investigations Operations Manual]. They know it exists," she said. "But I tell companies this all the time: If you really

want to know what's going on, read the IOM, read the regulations, read the QSIT manual, read the Compliance Program Guidance Manual, read the Regulatory Procedures Manual – read everything you can find."

However, there are few firms that have the money to hire someone to gather and review that information.

"It's usually your larger firms that have the resources to do that," Chase said. "You have to remember that the vast majority of medical device companies are medium-to-small firms. They are not big firms like Hospira and J&J. The majority are small- to medium-sized firms that don't have the resources. What they do is they hold their breath. They hope that when an investigator comes in and does an inspection they're going to be OK."

ture of them, would not necessarily strictly follow the QSIT program," she noted.

Weagraff said MDSAP is "QSIT on steroids," because whereas FDA allows for certain quality system subsystems to be skipped under QSIT, MDSAP's process is extremely thorough, charting an auditing map for investigators.

"MDSAP is looking at all four of the major subsystems. It's looking at management controls. It's looking at CAPA, design controls, production and process controls," she said. "In this case, the steroids are that instead of having an option to pick design controls or production and process controls like under QSIT, auditors are in fact doing them both – and even more – under MDSAP."

Mullen of device firm Cynosure said his firm underwent its first MDSAP audit in October, an experience he said was overwhelmingly positive. Cynosure's next MDSAP audit will come in March at the company's Hicksville, NY, facility. Mullen said he prefers an MDSAP audit to a QSIT inspection.

"QSIT can be non-predictive. Investigators can go all over the place. Who knows what the investigators are going to cover," Mullen said. "Whereas with MDSAP, you know the amount of time they're going to be there. And with QSIT you don't. I've had FDA investigators stay three weeks, and it's brutal."

MDSAP "certainly covers everything in QSIT, but it's also much more prescriptive," he said. "They have a guide they follow and they stick to it. In fact, we asked the MDSAP auditor to deviate – we wanted a section covered earlier because of the availability of people – and the auditor said he couldn't do that because MDSAP has to follow the sequence that is prescribed.

"MDSAP is more predictive than QSIT, even though QSIT is supposed to be predictive. We knew everything for MDSAP. We knew how to prepare everyone and get all the information ready for MDSAP," Mullen continued. "A lot of times investigators will call you up for a QSIT inspection and tell you the things they would like to see. But it's not a standard list. It's inspector-specific. 'I want the quality manual. I want this SOP. That SOP' – you never know. It's all over the map."

> "A lot of times investigators will call you up for a QSIT inspection and tell you the things they would like to see. But it's not a standard list. It's inspector-specific. 'I want the quality manual. I want this SOP. That SOP' – you never know. It's all over the map," Cynosure's Jon Mullen says.

MDSAP: QSIT 'ON STEROIDS'

But QSIT's effect on industry could be waning now that the Medical Device Single Audit Program is up, running, and gaining more manufacturer attention by the day.

MDSAP, created by the International Medical Device Regulators Forum, allows firms to undergo one audit by an accredited third party to satisfy quality regulations for the US, Canada, Brazil, Japan and Australia. Like QSIT, MDSAP is a process model.

"FDA is accepting the MDSAP audit reports as a substitute for a routine inspection. But they're not accepting MDSAP for for-cause or compliance follow-ups. They also will not accept MDSAP for pre-market approval applications," consultant Weagraff said.

"The movement away from the pure QSIT program could be because those types of inspections are for-cause, or compliance, or pre-market approval. And those types of inspections, simply due to the na-

QSIT – DESIGNED TO SAVE TIME – DOESN'T REALLY DO THAT

QSIT directs investigators to cover 38 core points related to CAPA, management controls, design controls, and production and process controls during a facility inspection.

"Those 38 points were what we thought were the key areas of a quality system back in 1999," QSIT coauthor Wells said. "Looking back, stupid things – such as, 'Did the firm create a quality policy and is it understood?' – could have been removed from QSIT."

That's because investigators "are wasting good auditing time asking questions that aren't necessarily pertinent; for example, investigators don't even know how to ask good questions when it comes to management controls," Wells said.

"When I left FDA there were the four subsystems in QSIT," he said. "But what the agency later proclaimed – after I left – was that investigators can do a [Level 1] 'CAPA plus one' inspection, which allows investigators to audit only two systems. That approach supposedly allows for a two- or three-day inspection."

Wells said FDA created CAPA plus one because it was trying to cram more inspections into an investigator's limited auditing time.

"Well, gosh, you can't really find anything in two or three days. It takes half a day just to figure out where the bathrooms are, and to get a product overview and an understanding of the building, the layout plan, and all those things," Wells said. "Now, I'm being rather facetious, but if the investigator is limited in time, then, dammit, they better focus the two days they are there on the most important things."

That's because "if you inspect in less time, you're just not going to get a fruitful inspection. You don't have time to dig. But investigators need that time to peel the onion back two or three layers. That's when FDA finds all the juicy stuff."

Although QSIT was set up to allow investigators to quickly inspect, it runs up against real-world issues that unfortunately cause delay, former FDAer Chase said.

"QSIT was designed so that if you did an abbreviated inspection, the most it should take the investigator would be one day for CAPA and one day for whatever the other subsystem is that's been chosen, and then maybe a day for tying up loose ends and closing out. But you must remember: That's an ideal world," she said.

"That's when the firm is cooperating, when they have the records available, when they give you the records, and when you're not finding major deviations," Chase noted.

"But there are many reasons why that doesn't work and why QSIT audits take longer than expected, such as the firm doesn't cooperate, the firm doesn't bring the investigator the adequate documents or the firm uses delay tactics," she said. "Or, the investigator might uncover a public health issue that will take time to process."

Ultimately, what Wells would like to see is an FDA that conducts fewer inspections, but schedules them to be twice as long.

"In other words, if they inspected for 10 days total, or if they had two auditors at the inspection, hell, they would get some good inspections done. But that's not going to fly because they want to inspect these firms every two years, yet the number of firms is increasing – and the number of investigators isn't," he said. "It is a dilemma that needs to be solved."

'NEW' QSIT BEING DRAFTED – BUT WHY?

Wells has been busy at work drafting a modern version of QSIT that allows for the most important parts of a quality system to be reviewed within a reasonable – yet appropriate – amount of time.

"QSIT was designed for FDA investigators to be quicker and more focused, but nowadays everybody is using it like it's the Bible for doing audits," he said. "But it's missing stuff. QSIT doesn't even ask about supplier controls. It was missing stuff from right after we launched it in 1999. Within two weeks, I started getting complaints that QSIT was missing certain things.

"So all I'm doing is trying to supplement it, I guess you could say, with stronger questions and more focus."

The "new" QSIT covers four quality system-related areas: post-market surveillance, design controls, supplier and process controls, and management controls. (See table above.)

"Instead of calling it 'CAPA,' I call my first subsection 'post-market surveillance,' which includes both CAPA and complaints. This new title lets auditors know that they're not just dealing with CAPA," Wells said. There are eight core points, or "expectations and guidance," in this section.

The updated technique includes a mix of bottom-up and top-down styles of auditing.

"In this new tool, it's probably more than an 80 percent bottom-up style of auditing," Wells said. "Industry might not like that because if you can get the investigators to focus on, say, procedures – which is a top-down approach – then they know everything will be OK because anyone and everyone can write a procedure. Nothing will be challenged."

The new QSIT is in a two-column format. The left-hand column includes FDA

Old QSIT Vs. Proposed New QSIT: QS Subsection Correlations

OLD		NEW
CAPA: 10 core points	Vs.	**Post-Market Surveillance**: 8 core points
Design Controls: 15 core points	Vs.	**Design Controls**: 8 core points
Production and Process Controls: 6 core points	Vs.	**Supplier and Process Controls**: 6 core points
Management Controls: 7 core points	Vs.	**Management Controls**: 4 core points

From New QSIT: Post-Market Surveillance

EXPECTATION		AUDIT GUIDANCE
Procedures: Both CAPA and complaint-handling procedures address all of the requirements of the FDA Quality System Regulation and Medical Device Reporting (MDR) regulation.	Top Down	Review of procedures, forms, work instructions and examples.
Trending: Appropriate statistical methods are used for complaint and CAPA trending. Software utilized for trending is adequate, appropriate and validated as necessary.	Bottom Up	Review trending of both complaints and CAPAs. Challenge the statistical thresholds for opening CAPAs. Confirm complaint frequency and severity are tied back to design risk analysis work (such as Failure Mode Effects Analysis).
Complaint Investigations: Post-market surveillance activities ensure that complaint-handling investigations are done to the necessary depth and based on the reported risk. Complaints are handled in a timely manner in order to allow for MDR considerations.	Bottom Up	Request printouts that show data, including the complaint allegations. Select samples based on risk. Review complaints that resulted in MDRs and some that did not result in MDRs. Determine their rationale for not reporting if you believe the complaint should have been reported. Determine adequacy (depth, timeliness and quality) of work done.

expectations; the column on the right offers audit guidance to ensure that expectations have been met.

In a Nov. 9 email to *Medtech Insight*, Wells explained: "I created the expectation column because I feel both the Quality System Regulation and the QSIT guidance fall short in explaining what is actually expected. While folks may argue this is best practice, I would argue that the agency expects these items."

He added: "The first column showing the expectation is a roadmap for industry. While it is a regurgitation of the regulations, in many instances it takes us further."

As an example, three core points on post-market surveillance from Well's new QSIT document are detailed in a table on p. 21.

Wells knows that FDA would probably never consider his new document as a QSIT replacement; rather, he hopes it will be used by manufacturers as they audit internally.

"Sadly, everybody relies on FDA to be their auditors. They take those audits to the bank and think Moses brought them down from the mountain, when in reality they need to clean up their own act, have their own audits, have their own processes," he said. "A lot of companies are using QSIT as their internal audit guide. I'm simply saying, 'Hey, you could do way better.'"

Despite there being fewer core points to cover under the new QSIT, audits "are not limited by four-and-a-half days. Firms could take as much time as they need to cover their quality system," Wells added, noting that he would be finished soon with the updated guide.

THREE QSIT AREAS THAT COULD BE BRIDGED NOW

While industry awaits Wells' new QSIT, there are gaps in the current version of the document that could be easily bridged without redoing the entire document.

During an interview, Wells pointed out three specific gaps that concern him:

Design Transfer. "I see this as a major gap in many companies. Often Industry does not understand that design control includes the need to ensure someone (internal to your company or external) has validated processes, qualified equipment, test methodologies and equipment, trained personnel, adequate work instructions, calibrated instruments, *et cetera*, so they can properly make the product.

"They can't throw the new design over the wall for someone else to manufacture. Product development people should own the process until the above items are completed and the manufacturing site has proven to be capable. This may slow down the product launch but it is essential. Lack of adequate design transfer is responsible for a lot of recalls, as well as injuries."

Management Controls. "A lot of people seem to think management controls is management review. It's actually much more than that. They also need quality goals and objectives so they can continually drive the organization into the area of improving their products and their quality system.

"Measurable outcomes should be expected, monitored and reported out in management review via scorecards and metric reports. Also, resources are only briefly mentioned in QSIT. Yet lack of resources (for example, when a company leans down their quality organization) can lead to massive compliance gaps, such as complaints and CAPAs not being reviewed, and Medical Device Reports not being filed. I believe QSIT would benefit by adding more specific questions on quality goals and objectives, and also on resources."

CAPA. "The second and third CAPA questions in QSIT are clear and well written in that sources of quality data should be analyzed as part of CAPA. But FDA doesn't go far enough, in my opinion, to drive companies to actually open CAPAs.

"For example, if you have a dysfunctional training process, you then need a CAPA to address why you have a dysfunctional training process. CAPA is too often used only for product issues. I see in industry that CAPAs are generally underutilized. Opening CAPAs forces the issues to be addressed. Management should be challenging the organization to not just close CAPAs, but to open CAPAs when they have gaps in their quality system. QSIT could sprinkle the CAPA question throughout the audit guide to ask if CAPAs are being opened."

From the editors of The Gray Sheet

CONTINUED FROM PAGE 16

could potentially better organize the FDA bureaucracy to develop rational-risk management policies. But with regards to approving products simply based on safety, he says FDA had done so in the past, until the Kefauver-Harris Amendments of 1962, which initiated the requirement in law for drugs to provide substantial evidence of effectiveness.

Shapiro pointed out that lawmakers have been trying to change the way FDA operates, in particular, trying to create a new regulatory paradigm that focuses more on post-market rather than pre-market data with passage of the 21st Century Cures Act, which is awaiting President Obama's signature.

"In the 21st Century Cures bill, Congress has just enacted statutory provisions trying to push FDA away from the traditional randomized clinical-trial model toward real-world clinical evidence and other new approaches to measuring safety and efficacy," he said. "There's a long way to go before we figure out the right balance between pre-market/post-market data."

He also added that a lot of investors and other experts are concerned FDA has not kept up with technological advancements in the medical device industry. While the agency functions as a gatekeeper for basic safety and effectiveness, Shapiro questions whether they truly are the best at deciding over the nuances of effectiveness.

If the reports pan out and O'Neill is appointed FDA commissioner, Shapiro says he would bring some new perspectives.

"He'll likely be coming at FDA regulation with a skeptical eye as an outsider, and I think it's appropriate," he said. "I think someone like this might ask some tough questions of a regulatory community that has become complacent."

However, Shapiro notes O'Neill would still have to work within the confines of Congress and US law.

"Nobody can just become FDA commissioner and change the system wholesale," he said. "There will be a lot of discussion. Ultimately, Congress has to approve."

Published online 12/8/16

Medtech Insight
Pharma intelligence | informa

advertise with us and take your business to the next level.

you won't believe the transformation

Contact our sales executive to learn about our various advertising opportunities available to you!

Christopher Keeling
+44 203 377 3183
christopher.keeling@informa.com
Customer Care: +1 888-670-8900 (USA)

medtech.pharmamedtechbi.com

Over 100 event types

Over 100 catalyst types

Over 5,000 products

Meddevicetracker
Pharma intelligence | informa

Double the Power

Meddevicetracker with Medtech Insight reports is a new interactive real-time source of in-depth medical technology market intelligence

Meddevicetracker brings you closer to the medtech market, helping you to:

- Identify upcoming device regulatory events/filings
- Search for medtech clinical trial starts and data
- Find historical and forecasted procedure volumes data
- Monitor drug delivery technologies and identify partnership opportunities
- Quantify the market size for devices or diseases
- Discover forecasted market share of devices by type
- Understand the device competitive landscape and identify unmet clinical needs

Request your free demo today:
please visit - **www.meddevicetracker.com**