White Paper

Five Trends Transforming the Medical Device Industry in 2015

MasterControl™
Compliance Accelerated

Introduction

Brace yourself for another year of opportunities and challenges in the medical device industry. For 2014, we predicted that longer life expectancies, emerging markets, increased regulatory scrutiny and health care reform would drive industry change. As we move into 2015, we see many of those trends continuing to evolve, and some exciting new trends emerging. Disruptive technologies like 3-D printing and mobile health applications are prompting regulators to re-examine their roles, leading to new regulatory frameworks and clarified rules. Consumers are demanding more transparency and convenience but are also concerned about the security of their medical information and devices. Investors and stakeholders are paying closer attention to reimbursement policy, which could limit innovation and access to life-saving products. A wired, patient-centric device market is taking shape, and the industry must learn to adapt—quickly. The following pages highlight five trends device manufacturers would be wise to follow closely this year.

Trend #1: Three-Dimensional (3-D) Printing Will Revolutionize Personalized Medicine

Imagine a time when a clinician can modify and manufacture an implant sized for a particular patient on-demand in a health care facility—or print a human organ as easily as a paper document. As futuristic as it sounds, that time is not far off, according to scientists who continue to find new and truly mind-blowing ways to apply three-dimensional (3-D) printing techniques to the medical field.

As its name suggests, 3-D printing, also known as additive manufacturing, is a process in which objects are made by fusing or depositing materials, such as plastic, ceramics or even living cells, in layers to produce a 3-D object. The concept is not new; 3-D printing technology has existed in some form since the 1980s. However, what was once considered a niche manufacturing process has blossomed into a multi-billion-dollar industry, responsible for fabricating everything from wristwatches to airplane parts.

Until recently, though, 3-D printing had been used sparingly in the device industry, primarily to create surgical guides and prototypes or products that required only simple materials such as polymers, acrylics or ceramics. A lack of qualified materials prevented applications from being used in and around the body. The technology was also considered too slow and expensive for widespread prototyping and design work. However, with the new generation of faster, more accurate 3-D printers, these limitations have all but disappeared. Today, device makers are using 3-D printers to build clinical trial-ready devices in-house to check everything from form, fit and function to manufacturability. In fact, some of the most exciting applications of this disruptive technology are occurring in the medical device space.

Customization of Medical Devices

The greatest advantage 3-D printing offers device manufacturers is the ability to fabricate customized medical products and equipment. Custom-made implants, prosthetics, fixtures and surgical tools can significantly reduce the time required for surgery, as well as patient recovery time and follow-up care. This in turn reduces health care costs. The technology is transforming the way medical care is practiced and delivered, shifting from a reactive population-based model to a customized one, typically referred to as *personalized medicine*.

Personalized medicine targets individualized treatment and care based on personal and genetic variation, taking into consideration the patient's genetic make-up, key biomarkers, treatment history, environmental factors and behavior preferences. The treatment model has already had a positive impact on clinical research and patient care, particularly in the treatment of breast cancer, melanoma and cardiovascular disease. According to PricewaterhouseCoopers, the core diagnostic and therapeutic segment of the personalized medicine market, which is comprised primarily of pharmaceutical, medical device and diagnostic companies, is expected to reach $42 billion this year.[1] However, the full realization of personalized medicine relies on the continued improvement and acceptance of disruptive technologies like 3-D printing among health care professionals, regulators, policy makers and insurers.

Additional Benefits of 3-D Printing

Three-dimensional printing enables mass customization, in that multiple individualized items can be produced simultaneously while improving manufacturing productivity. Early adopters of 3-D printing for the mass production of customized medical devices include dental laboratories and hearing aid manufacturers. In fact, the hearing aid industry boasts the highest installed base of customized final consumer devices that have been produced using 3-D printers.

As the technology becomes more cost-effective for small production runs, the use of 3-D printing in mass device production is rapidly expanding. This is especially true for small-sized standard implants and prosthetics used to treat spinal and craniofacial disorders.[2] Three-dimensional printing technology is much faster than traditional (i.e., subtractive) methods of making prosthetics and implants. It cost less, too, with the first item being as inexpensive to print as the last. This is especially advantageous for device companies that have low production volumes or produce parts or products that are highly intricate or require frequent modifications.

The nature of 3-D printing data files also offers an unprecedented opportunity for global collaboration among researchers who can now access downloadable .stl files available in open-source databases. In 2014, the National Institutes of Health (NIH) established the NIH 3D Print Exchange (3dprint.nih.gov) to promote open-source sharing of 3-D printable files for medical and anatomical models. The Exchange allows users to generate high-quality and scientifically-accurate 3-D printable models in minutes, simply by uploading a file or typing in a database accession code.[3] Design sharing is expected to accelerate innovation and deliver life-saving products to market sooner.

Challenges 3-D Printing Poses to Manufacturers and Regulators

Clearly 3-D printing has the potential to revolutionize the device industry, but the technology is not without drawbacks. Three-dimensional printers can copy almost anything, making products highly vulnerable to counterfeiting. Some experts predict that one day all products will be produced locally, if not in households, making manufacturing as we know it obsolete. Others argue that the technology will have to improve significantly before a 3-D printer is capable of producing realistic fakes made from a single material, let alone composite products made of several different materials, as is the case with most medical devices.

There are a myriad of regulation challenges to confront, as well, acknowledged Steven Pollack, the director of FDA's Office of Science and Engineering Laboratories. For example, in a traditional manufacturing setting, design controls are in place that may be lacking in a 3-D setting. Devices manufactured using 3-D printers may also require additional or different testing than what is performed on products produced using traditional manufacturing techniques. Although 3-D printing techniques have different technical considerations than standard manufacturing, devices constructed using additive manufacturing techniques are subject to the same regulatory review standards as traditionally manufactured devices.[4]

Validation and Design Control are the Biggest Areas of Concern

In October 2013, the FDA released a 63-page report, titled "Paving the Way for Personalized Medicine: FDA's Role in a New Era of Medical Product Development," which is available at www.fda.gov. The report discussed 3-D printing and other technological advancements that have the potential to disrupt the regulatory status quo. The FDA has also created an additive manufacturing working group to explore some of the design and testing challenges posed by the revolutionary technology. On October 8-9, 2014, the agency held a 3-D printing workshop for industry stakeholders, including OEMs, device manufacturers, testing labs, hospitals, and government agencies. The majority of participants agreed that paying close attention to quality control and process validation was essential to their future success.[5]

As the aging developed world population continues to grow so does the consumer demand for medical devices, particularly diagnostic equipment and other devices that focus on disease prevention. Three-dimensional printing may make the development of such devices feasible that previously was not. The fact that the FDA is addressing 3-D printing at this early stage of its adoption in medical devices should convince manufacturers to pay close attention to it in 2015.

Trend #2: Mobile Health Applications Will Become Pivotal Instruments in Patient Care

Mobile health, or mHealth, has gained significant momentum over the past couple of years, and it will continue to influence product development in 2015. Millennials raised on technology are providing device makers with the unprecedented opportunity to sell directly to consumers in the form of wearable devices and mobile health applications that allow patients and physicians to interact clinically from different locations. The popularity of mHealth tools has been fueled by the growth of the smartphone industry.

More than half a billion smartphone users are expected to be using mobile health apps this year; that number is projected to climb to more than 1.7 billion by 2018.[6] Clinicians, who are under pressure to reduce costs and improve outcomes, are in favor of using mHealth tools, as well. Survey results released by the PwC Health Research Institute (HRI) indicate that nearly 90 percent of U.S. clinicians think mobile apps will become essential to patient health management over the next five years.[7] Seventy-four percent of the HRI respondents said they would be willing to use data streamed from a mobile app/device to check for ear infection; 53 percent were in favor of using a mobile app/device to analyze urine, and 20 percent have already prescribed nutrition and weight loss apps.[8]

UK Doctors Have Been Prescribing mHealth Apps Since 2012

The mHealth adoption curve has been slower in the U.S. than in other developed nations. In early 2012, the U.K. Department of Health started encouraging physicians to direct their patients to use mobile apps in an effort to save the National Health Services (NHS) "millions of pounds" in unnecessary doctor visits and to connect people to health services more efficiently.[9] mHealth adoption has been so successful in the U.K. that the NHS has created a curated database of government-approved mobile mental health apps on its NHS Choices website. The NHS plans to expand the database to other health areas in the future.[10]

New Lines of Revenue

Mobile app development is particularly attractive to start-ups, the current market dominators, because apps typically take less time to bring to market and require less, or different, regulatory scrutiny. This is particularly true for apps positioned as wellness devices rather than medical devices. Wellness apps are not regulated, so they allow device makers to expand their product offerings and generate new lines of revenue quickly. However, it can be difficult to determine if a mobile app falls inside or outside the realm of FDA authority, i.e., whether it meets the definition of a medical device under section 201(h) of the Federal Food, Drug, and Cosmetic Act (FD&C Act).

In September 2013, the FDA issued a guidance document explaining how it intended to regulate the rapid proliferation of mobile health apps. The final guidance, "Mobile Medical Applications: Guidance for Food and Drug Administration Staff," was issued on February 9, 2015. According the guidance, the "intended use" of the device will determine whether the FDA will regulate it. "When the intended use of a mobile app is for the diagnosis of disease or other conditions, or the cure, mitigation, treatment, or prevention of disease, or is intended to affect the structure or any function of the body of the man, the mobile app is a device."[11]

Mobile health apps that meet the criteria of a device but pose a low risk to consumers are subject to "enforcement discretion," meaning the FDA will not enforce requirements under the FD&C Act. Mobile apps that use GPS location information to alert asthmatics of environmental conditions that may cause asthma symptoms or alert an addiction patient when near a pre-identified, high-risk location are examples of apps that fall under "enforcement discretion."[12]

A current list of examples of regulated apps, apps subject to enforcement discretion and unregulated apps is available at www.fda.gov. Device makers can also email a 513(g) request to the FDA at mobilemedicalapps@fda.hhs.gov, and ask for a formal determination of whether a mobile app falls under regulatory jurisdiction. It takes approximately 60 days to receive a response.

Only Apps That Add "Real Value" Will Attract Investors

Although mobile apps are all the rage, some experts suggest that the mobile health app market may be reaching a tipping point in terms of saturation. They emphasize the need to provide real value, not just novelty or convenience. "Mobile health apps are a hot trend at the moment, but the market is highly saturated, with very few avenues to distribute them," said Joe Hage, administrator of LinkedIn's Medical Devices Group, which has more than 275,000 members. "Apps that are simply designed to make life easier aren't going to get funded. Investors are taking due diligence very seriously. App developers must be able to demonstrate real value."

With more than 50,000 free and nearly-free app products available, and smartphone real estate relatively sparse, the competition is stiff. Wellness and other nonregulated apps will enter the market faster and at a lower price point, but they may get lost in an overly-saturated market. Apps that add real value are those that provide diagnostic and treatment capabilities, features that will require regulatory approval. Although these apps will take longer to bring to market, regulatory approval may provide a competitive edge, according to the HRI survey. "Twenty percent of respondents acknowledged that FDA approval was very important in their decision to purchase or use a mobile app.[13] Similarly, 26% of physicians said FDA approval was most important when deciding to prescribe apps."[14] Successful device and software manufacturers should bear this in mind in 2015.

Trend #3: Reimbursement Approval Will Rival Regulatory Approval as a Business Goal

Reimbursement will be a driving factor in securing venture funding not only for mHealth technologies but also for medical devices across the board in 2015. In addition to clinical utility, device manufacturers are now required to demonstrate the economic benefits of their product in producing cost-effective outcomes, increasing pressure in an already risk-averse investor environment. In its 2015 Medical Device Industry Survey, Emergo asked 636 presidents, CEOs and managing directors of medical device companies what issues were keeping them up at night, and reimbursement challenges ranked in the top three.[15]

Reimbursement, as it applies to medical devices, is defined as the payment a third party public or private insurer pays a health care provider for costs or payments the provider incurred while using a medical device or performing a procedure. Whether a device or procedure is covered as reimbursable, and at what amount, can have a significant impact on a provider's ability to access a particular technology, as well a manufacturer's ability (or willingness) to provide it. If coverage is uncertain, it is difficult for the manufacturer to predict whether an investment in a new technology will provide sufficient returns. This lack of predictability is an obvious barrier to securing venture funding. Moreover, it compromises innovation and limits patient access to advanced technologies and solutions.

"Reimbursement is the number one issue on investors' minds, and one of the first things companies think about when developing products," said Robert Packard, a regulatory consultant and trainer with two decades of experience in the medical device industry. "Ten years ago, investors didn't know—or probably care—what CPT [current procedural terminology] codes were, but today they are far more savvy. In some ways, it's stifling innovation, and it's definitely increasing the cost of product development by forcing more companies to conduct clinical trials."

Top Reimbursement Policy Challenges

Reimbursement challenges vary by country, so it is important for device companies to investigate the reimbursement environment of a particular market before investing in product development. Still, there are some common challenges many countries share.

One major reimbursement challenge is the misalignment of reimbursement rates and the value of medical technologies. In most countries, reimbursement rates are set based on standing formulas (i.e., cost-based) that are applied to device or procedure types, rather than individual manufacturer's technology or features (i.e., value-based).[16] This often prevents companies from developing (and patients from accessing) more advanced technologies which can actually lower costs and improve outcomes in the long run. The future of medical innovation depends on governments adopting reimbursement policies that are value-based rather than cost-based.

As the aging population continues to expand, governments worldwide are trying to contain health care costs by cutting reimbursement amounts. Some governments have cut back on reimbursement for medical devices, which typically account for six to seven percent of overall health care spending, according to the Global Medical Technology Alliance (GMTA).[17] In the U.S., Congress has cut medical imaging reimbursement 13 times since 2005, resulting in a 35 percent decline in revenue for the industry—despite evidence that shows the economic and clinical value of medical imaging. For example, a study in the journal *Radiology* found that every $1 spent on imaging decreases hospital stays by one day, contributing to a cost savings of $1,172 a day. [18]

Another challenge is the increased burden to provide evidence of both the clinical and economic effectiveness (i.e., the value) of a device as part of the coverage decision. While more stringent coverage requirements are understandable in this age of health care reform, the increased burden may deter companies from investing in new technologies that could lead to better health outcomes.

Planning for Reimbursement Success

Although reimbursement was once considered the sole responsibility of the provider, times have changed. Today, manufacturers must participate in—or even lead—the reimbursement process to achieve sales success. Too often, reimbursement questions such as "who will pay for this new device?" and "how much?" are considered too late in the development process. To prevent reimbursement issues from impacting financing goals or stalling innovation, device makers must develop a well-planned reimbursement strategy in parallel with their regulatory and clinical strategies. This may prove difficult for device makers that have become accustomed to focusing on achieving 501k clearance. Given the time and effort it takes to obtain approval to market a device, some level of tunnel vision is understandable. However, in the current climate, reimbursement approval is just as important as regulatory approval.

Payment is the reward for the hard work and effort it took to get the device cleared for commercial sale. Generating revenue sooner rather than later is often critical for start-ups and small device companies after a lengthy regulatory approval process. Again, proper planning is the key to jumpstarting sales growth and market adoption efforts. Collecting both Class 1 (RCTs—random control trials) and Class 2 (prospective registries, longitudinal studies, case-control studies) post-approval data is essential, and can provide valuable information that can be used to create a compelling sales and marketing message. Equally important, yet often overlooked, is having a publication plan for disseminating the outcomes data, ideally in peer-reviewed journal publications or at medical conferences. Again, this requires strategic planning and should be considered early in the development process.

The Sunshine Act/Open Payments Program

Regardless of reimbursement, a device will not sell unless it is supported by physicians and accepted by the medical community at large. While doctors are not allowed to be paid for authorship or to act as a speaker on a device company's behalf, companies can pay expenses for meeting attendance, development work, and other advisory activities. The relationship between physicians and device companies is necessary to advance innovation and patient care, but it can create bias or conflicts of interests. It also creates regulatory concerns.

In February 2013, the U.S. Centers for Medicare & Medicaid Services (CMS) released final regulations to implement the Physicians Payments Sunshine Act, which was part of the health care reform bill adopted in March 2010. The Sunshine Act (now called Open Payments) requires all manufacturers that obtain reimbursement for their products through Medicare to report how much they spend annually on physician and continuing education activities. Its enactment has direct implications for medical communications and clinical data collection activities that are necessary to ensure sales. Companies that fail to comply with the program risk incurring stiff financial penalties (up to $1,150,000), legal conflicts and brand damage from consumers who are demanding more transparency in life science companies' business and clinical operations.

The French Sunshine Act ("FSA"), also known as *Loi Bertrand*, was adopted on December 29, 2011, and the final decree was issued on May 21, 2013. Though strides were made to repeal the law, in March 2015, RAPS reported that France has plans to expand the scope of the reporting requirements to include any non-service payments made to health care professionals in excess of €10 ($11). If adopted, these changes will bring France more in line with the European Federation of Pharmaceutical Industries and Associations (EFPIA) Disclosure Code, which is discussed in greater detail on page 8.[19]

The Shift Toward Value-based Reimbursement

It is no longer sufficient to demonstrate medical need or marginal product benefits for new product launches. Even having a superior product or pioneering a new technology will not guarantee reimbursement success. Health care reform efforts such as The Affordable Care Act (ACA) are transitioning the industry from a volume-based to value-based care model, which links reimbursement to quality, better care and cost containment. As part of this transition, medical device companies will be required to provide evidence of real-world value and positive outcomes. Products that fail to provide such evidence will struggle to generate investor support or attain reimbursement. The bar for demonstrating value is high—and will continue to rise throughout 2015. Crafting a reimbursement strategy early in the product development process will ensure that great technology is not only available, but also accessible to the patients who need it most.

Trend #4: 2015 Will Bring a Stronger Focus on Cybersecurity in Medical Devices

The recent security breach of health insurer Anthem Inc. should be a wake-up call to the health care industry—one that is long overdue, according to security experts. On February 5, 2015, hackers stole the social security numbers and personal information of 80 million Anthem members and employees, leaving them vulnerable to identity theft and blackmail.[20] While Anthem may be one of the biggest health care companies to suffer a breach, it certainly isn't the first. In October 2014, the Department of Homeland Security investigated more than 20 suspected cases of cyberthreat in hospital equipment and medical devices, bringing some well-known health care giants under scrutiny.[21] That same month, the FDA published a cybersecurity guidance for medical device makers, outlining the security measures developers should build into their products when seeking approval for a new device.

The final guidance, titled "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices," recommends that manufacturers consider cybersecurity risks as part of the design and development of a medical device. Manufacturers should submit documentation about the risks identified, and the controls instituted to lessen those risks. The guidance also recommends that manufacturers submit their plans for providing patches and updates to operating systems and medical software.[22] By carefully considering possible cybersecurity risks while designing medical devices, and having a plan to manage system or software updates, the FDA believes manufacturers can reduce the vulnerability in their medical devices.

"Devices are becoming more interconnected and interoperable, which is great for patients and providers in so many ways," said Hage, who is also the founder and CEO of Medical Marcom. "However, it's important to remember that increased connectivity leads to increased vulnerability and risk. There's no getting around it."

How Vulnerable Are Devices?

A December 2012 episode of the television show "Homeland" featured a storyline in which the Vice President of the U.S. was killed by a terrorists who hacked into his pacemaker remotely. Viewers were horrified and questioned if the plot was plausible in real life—or something dreamed up by Hollywood. Popular magazines, such as *Forbes* and *The Atlantic*, wrote articles about the vulnerabilities in internet-connected implanted medical devices. Talk radio programs were inundated with assassination-by-pacemaker-related calls. A TED talk was created. Even a real, albeit former, U.S. vice president weighed in on the topic.

During a 2013 television interview with "60 Minutes," Dick Cheney, who served as the 46th vice president of the U.S. (2001-2009), admitted that he had his doctor disable the remote access to his pacemaker, which he had implanted in 2007, because he had legitimate concerns about the threat. (A pacemaker or defibrillator is equipped with remote control abilities for a doctor to make adjustments using a computer program.) Talking about the "Homeland" plot, Cheney said, "I found this credible. I know from the experience we had, and the necessity for adjusting my own device, that it was an accurate portrayal of what was possible."[23]

Cheney was right to be concerned. New Zealand hacker and security expert Barnaby Jack developed software that allowed him to send remotely an electric shock to anyone wearing a pacemaker within a 50-foot radius. Equally unnerving was the system he developed that could manipulate any insulin pump within 300 feet to distribute too much or too little insulin, sending the diabetic into hypoglycemic shock. According to Jack, manipulating sophisticated medical equipment is not as difficult as one might think. "It does take a specialized skill, but with more and more security research concentrating on embedded devices, the skill set required is becoming more common. It probably took me around six months, from reverse engineering and finding the flaws through to developing software to exploit the vulnerabilities," he said in a 2013 interview with *Vice* magazine.[24]

Updated Software Lowers the Risk of Cybercrime

Contributing to the risk is the fact that hospitals and other providers do not upgrade their software as often as they should because they fear falling out of FDA compliance. This means that important "everyday" medical devices, such as health and blood pressure monitors, can be manipulated to display incorrect vital signs and cause doctors to provide incorrect medical care. Frightening, yes, but most cybersecurity experts agree that hackers are more interested in stealing records that reprogramming pacemakers.

Jay Radcliffe, a security researcher who hacks into medical devices for a living, estimates that medical-identity information is worth 10 times more than credit-card information—about $5 to $10 per record—on the black market. In comparison, credit-card information is worth only 50 cents per account.[25] Stolen medical information can be used to apply for credit, fake insurance claims, or to buy and resell drugs and medical equipment for profit. Breaches are expensive. Eleven days after Anthem went public with its security breach, the insurer began offering free, two-year identity repair and identity monitoring services for the current and former customers and employees whose personal information might have been accessed, costing Anthem millions.[26]

The Future of Medical Device Security

The proliferation of electronic medical records (EMR), networked devices, mHealth applications, and cloud-based technologies has added to the complexity of information management. In this new digitized health economy, balancing convenience, safety and privacy will be an ongoing challenge. Moreover, it is likely to be consumers more than regulators who will be calling for greater cybercrime vigilance and increased data security.

According to PricewaterhouseCoopers, U.S. consumers have expressed a clear preference for privacy over convenience regarding medical testing and imaging results, personal information about a patient's diagnosis, and his or her drug prescriptions. Health experts worry that the fear of a data breach will have a negative impact on doctor-patient communication, which could compromise patient safety and care. Fifty-six percent of consumers said that concerns about medical data security would affect how much information they would disclose about their medical history and/or conditions; 51 percent said it would affect their decisions to participate in clinical trials.[27]

To put consumers' minds at ease, device makers will be required to meet/answer a myriad of security requirements/questions: Can the device be encrypted? Is there a unique identification for users? What happens in a case of emergency? If the vendor is hosting the device, what does their system look like in terms of firewalls and other protections? Will the manufacturer provide up-to-date security patches and frequent upgrades? Of the more than 6,500 device makers in the U.S. alone, roughly 80 percent have under 50 employees and cannot afford to invest in a security expert.[28]

Earlier this year, the Federal Trade Commission (FTC) released a report, titled "Internet of Things: Privacy & Security in a Connected World," to provide companies with insight into the FTC's consumer privacy and data security expectations for the rapidly growing market of Internet-connected products, commonly called the Internet of Things (IoT). The report offers six recommendations that IoT-style devices, which include medical and clinical devices, need to maintain good security. One recommendation is to retain service providers and vendors that are capable of maintaining reasonable security. [29]

The FDA and FTC guidelines are consistent, suggesting that medical cybersecurity is not a feature or function to be addressed at the end of the design process. Device companies that treat it as such are likely to build devices that get their consumers' personal data hacked, end up in the news, and, eventually, out of business. Conversely, device companies that take a proactive approach to cybersecurity, by budgeting for and building it into their design process, will be able to use it as a competitive differentiator.

Trend #5: The Push for Global Transparency Will Continue to Increase

Transparency has been a hot topic in life science circles in recent years. So hot, in fact, that it has almost become a buzzword, which implies that it lacks real substance or staying power. Transparency advocates, who are pushing to make health industry data—everything from clinical trial results to procedure pricing information—more accessible, would disagree.

The transparency movement sweeping the industry is not just about uncovering financial conflicts of interest in medical and clinical practice vis-à-vis the Sunshine Act/Open Payments. True transparency, advocates argue, will result in better clinical trials, happier patients, improved outcomes and lower costs of care. Moreover, they point out that transparency is inevitable in today's consumer-centric information age—and it's accelerating. The movement has already led to widespread changes in the U.S. and abroad, and it is likely to continue to dominate conversations throughout 2015 and beyond.

Study Reports One Quarter of Clinical Trial Data Withheld

Medical researchers claim that a substantial amount of clinical trial data goes unpublished, robbing researchers of valuable information and raising ethical concerns about the treatment of trial participants. As an example, the *British Medical Journal* cited a 2013 study in which of a group of researchers at Cooper Medical School of Rowan University in Camden, New Jersey, examined 585 registered clinical trials that had been completed nearly five years prior. The group found that 29 percent of the trial data sets, with an estimated enrollment of almost 300,000 participants, went unpublished.[30]

"The non-publication of trial data…violates an ethical obligation that investigators have towards study participants," said the Cooper team. "When trial data remains unpublished, the societal benefit that may have motivated someone to enroll in a study remains unrealized."[31]

The AllTrials Petition

Of the many open data initiatives making the rounds, one that is gaining momentum is the AllTrials petition. As of April 2015, more than 550 government regulatory bodies, clinicians and organizations, including GlaxoSmithKline, had signed the petition, which calls for all past and present clinical trials to be registered and their full methods and summary results to be reported. Failure to do so, according to the AllTrials website, violates the principles of the Declaration of Helsinki, which states that every investigator conducting a clinical trial should register the trial and report its result. Moreover, AllTrials argues that withholding trial results—even negative, null and inconclusive findings—can lead to poor treatment decisions and duplicated research efforts and delay the process of finding positive results. Some investigators and life science companies contend that it is often difficult to find a home to publish null or negative findings. Indeed publication bias, along with the idea that all results are valuable, led to the creation of the *Journal of Negative Results in BioMedicine* in 2002.[32] The Journal was one of the first platforms to push for publication and discussion of null, nonconfirmatory findings.

Other Open Data Initiatives

Large medical device and pharmaceutical manufacturers are contributing clinical trial data sets to Project Data Sphere, the Yale University Open Data Access (YODA) Project, and other programs. As of February 13, 2015, YODA had 112 trials available from the pharmaceutical, medical device, and diagnostics businesses of Johnson & Johnson, as well as Medtronic, Inc. Investigators can submit their data requests on YODA's website (yoda.yale.edu). "Sharing data from clinical trials leads to greater insights in medicine. This agreement with the YODA Project underscores Johnson & Johnson's commitment to responsibly share clinical trial data with researchers in a way that we believe advances medical science and public health," said Dr. Joanne Waldstreicher, chief medical officer of Johnson & Johnson. [33]

Regulators are on board, too. The European Medicines Agency (EMA) will commence publishing clinical trial data used to support the approval and authorization of new drugs in Europe in 2015. Moreover, the EMA has announced plans to release anonymized patient data in the future. The OpenFDA Initiative, launched last year, provides a public database for analyzing drug and medical device adverse events, recalls and labeling information. In the past, this information was "difficult for industry to access and to use," acknowledged Taha A. Kass-Hout, M.D., the FDA's chief health informatics officer and director of its Office of Informatics and Technology Innovation. "Pharmaceutical companies, for example, sent hundreds of Freedom of Information Act (FOIA) requests to FDA every year because that has been one of the ways they could get this data. Other methods called for downloading large amounts of files encoded in a variety of formats or not fully documented, or using a website to point-and-click and browse through a database—all slow and labor-intensive processes."[34]

Self-regulation in Europe, Australia and Japan

The pharmaceutical industry in Europe has taken an active role in developing a self-regulatory system of transparency. In June 2013, the EFPIA, comprised of 33 national European member associations and forty pharmaceutical companies, adopted the "EFPIA Code on Disclosure of Transfers of Value from Pharmaceutical Companies to Healthcare Professionals and Healthcare Organizations" ("Disclosure Code"). The Disclosure Code requires members to publicly disclose, in 2016, many of their 2015 financial interactions with health care professionals (HCPs) and health care organizations (HCOs)[35]. Medicines Australia, whose members deliver 86 percent of the countries pharmaceuticals, hopes to have a similar self-reporting system in place by 2016.

In Latin America, Africa and the Middle East, the transparency movement appears to be in its infancy. Those regions lack both government-driven legislations (e.g., Sunshine Laws/Acts of France and the U.S.) and self-regulatory codes, as does Asia, with the exception of Japan. In Japan, both pharmaceutical and medical device industry groups have self-reporting requirements for their members.

The medical device industry seems to be lagging behind the pharmaceutical industry when it comes to self-regulation. Though Eucomed, AdvaMed's European counterpart, "strongly supports transparency as a broad principle," its members are not, at this time, subject to EFPIA-like reporting requirements.

Implications for Device Makers

The ever-expanding movement toward greater transparency with respect to pricing and financial interactions between industry and providers continues to pick up steam. Life science companies around the world have been forced to confront both government-imposed and self-imposed reporting obligations, and further enforcement is anticipated. Data sharing and reporting across companies and continents is quickly becoming a reality. Medical device companies would be wise to invest in data sharing and analytics software that will help them gain a competitive edge.

How MasterControl Can Help the Medical Device Industry

Hundreds of device companies throughout the world use MasterControl's quality and compliance software to comply with FDA 21 CFR parts 820 and 11, the Medical Devices Directive (MDD) 2007/47/EC, ISO 13485 and 14971, and other requirements and standards used in the medical device industry.

An end-to-end solution, MasterControl provides an effective framework for a company's quality management system (QMS) by automating and connecting all system processes (everything from design control to audit), and providing a web-based, centralized repository for all documentation and records. The solution suite can help device manufactures improve operational efficiency, agility and achieve continuous compliance.

In addition to automation, MasterControl offers medical device companies three key advantages:

- **Mobile Access**—MasterControl allows users to access critical compliance-centric documents and information and perform tasks using a tablet or a smartphone. Mobile access offers greater flexibility for users and helps boost overall efficiency and productivity.

- **Cloud-Based Services**—For companies that want to avoid the cost-prohibitive upfront investment typically associated with purchasing an on-premise QMS system, MasterControl offers private cloud-based services. MasterControl's cloud-based QMS provides the same robust system in a secure environment without the need for a large IT staff. Companies can deploy faster, a benefit that can improve compliance and deliver a much faster and higher ROI.

- **MasterControl Spark!™**—Fully loaded and fully validated, Spark is a hosted product package targeted at companies with fewer than 50 employees. These companies have the same rigorous quality, regulatory, and document control needs as large companies but they typically have less money, fewer resources, and tighter timelines. Spark was specially built to fit the distinctive requirements of these emergent companies and to get their high-quality products to more people sooner.

MasterControl offers the following modules:

MasterControl Documents: For many manufacturers of medical device and diagnostic equipment, the MasterControl Documents module typically serves as the foundation for building a robust enterprise QMS. It allows users to track, search, retrieve, route, review, and approve documents electronically, increasing efficiency while simultaneously reducing the possibility of human error and lost documentation. Because the module has been designed to consolidate document control with other quality system management processes, such as design control, audit management, CAPA, risk management, supplier management, and bill of materials (BOM) management, it provides the enhanced visibility medical device managers need to react and adapt to the latest business and industry trends.

MasterControl Training: Medical device manufacturers use the MasterControl Training module to automate the distribution and monitoring of training tasks. Because enhanced regulatory oversight is expected to continue to increase throughout the medical device industry in the coming years, implementing a robust training module is critical to ensuring that all employees are properly trained to the latest standards and regulations and internal company procedures.

MasterControl CAPA: Medical device manufacturers need to maintain control of their CAPA processes to avoid regulatory penalties. MasterControl CAPA is a closed-loop, easy to use solution that streamlines the management of quality events from root cause investigation through the implementation of the preventive action.

MasterControl Audit: Medical device manufacturers use audits to prove their processes and procedures are in compliance with SOPs and regulatory standards, mitigate risks, manage supplier quality, and increase organizational transparency. The MasterControl Audit module is robust enough to handle all of these tasks. It offers robust reporting tools and the capability to connect the audit management process with other critical quality processes.

MasterControl Risk: In the medical device industry, risk management has become an integral part of the design, development, and production processes. Risk management is applicable to all types of medical device equipment, and most regulatory bodies require evidence of its application. The MasterControl Risk module provides a single platform for all risk-centric activities and documentation to help drive an organization's compliance goals.

MasterControl Supplier: This "one-stop shopping" solution integrates supplier management with the quality management system and provides a single repository for all supplier quality data and documentation. It allows users to create scorecards for the evaluation of suppliers. It also provides robust tools for tracking and trending supplier quality events such as deviations and supplier quality action reports (SCARs).

MasterControl BOM: The bill of materials (BOM) has always been critical to a medical device company's overall success, but never more so than now. As outsourcing and expansion into emerging markets continue to increase the number of suppliers involved in the manufacturing of a particular device, the margin for error also increases. MasterControl BOMs "where-used" feature displays exactly where a part is used across multiple BOMs, permitting users to determine the impact of a single part change and updating subsequent changes where needed.

Conclusion

The medical device industry, which is known for producing life-saving innovations that benefit millions of people worldwide, is facing unprecedented challenges in 2015, but many opportunities as well. To succeed, device manufacturers must understand and learn to navigate the industry's most pressing trends: disruptive technologies like 3-D printing; the proliferation of mHealth applications; a risk-averse investor climate, which is besieged by reimbursement challenges; cybersecurity threats; and the increasing push for transparency from government, health care professionals and consumers.

Patients are becoming the industry's new customer. The number of approved portable medical devices on patients' smartphones is facilitating diagnosis and treatment but complicating product design (developers must learn to design for consumers, not physicians) and making products more vulnerable to cybercrime. These new products must demonstrate not only clinical efficacy, but also real value in order to secure reimbursement and attract investors. Regulators are struggling to ensure device

safety and efficacy—without hindering innovation. New transparency initiatives targeting clinical trial data sets are increasing, and device makers must learn to deal with the paradigm shift. These matters and others will be important as 2015 unfolds. Of course, one "trend" that will never go away is the need for compliance, and 2015 is shaping up to be the year of global medical device regulation harmonization. An automated QMS can help device manufacturers ensure that they are operating efficiently and compliantly, and give manufacturers the analytics and reporting tools they need to gain a competitive advantage in 2015.

Endnotes:

[1] "$232 Billion Personalized Medicine Market to Grow 11 Percent Annually, Says PricewaterhouseCoopers," PR Newswire. (http://www.prnewswire.com/news-releases/232-billion-personalized-medicine-market-to-grow-11-percent-annually-says-pricewaterhousecoopers-78751072.html) Accessed March 31, 2015.

[2] Ventola, C. Lee, "Medical Applications for 3D Printing: Current and Projected Uses," Pharmacy and Therapeutics, October 2014. (http://www.ptcommunity.com/system/files/pdf/ptj3910704.pdf)

[3] National Institutes of Health. http://3dprint.nih.gov

[4] Sparrow, Norbert, "An FDA Perspective on the Use of 3D Printing in Medical Applications," Plastics Today, January 5, 2015. (http://www.plasticstoday.com/articles/FDA-perspective-on-use-3D-printing-medical-applications-150105)

[5] Leonard, Shana, "FDA Grapples with Future Regulation of 3-D Printed Medical Devices," MD+DI, June 13, 2014. (http://www.mddionline.com/article/fda-grapples-future-regulation-3-d-printed-medical-devices-140613)

[6] Hartford, Jamie, "Will FDA Regulate Your Mobil Medical App?" MD+DI, August 6, 2014. (http://www.mddionline.com/article/will-fda-regulate-your-mobile-medical-app-08-06-2014)

[7] PWC Health Research Institute, "Clinician Survey," 2014.

[8] Ibid.

[9] Dolan, Brian, "UK to Encourage Doctors to Prescribe Health Apps," February 22, 2012. (http://mobihealthnews.com/16401/uk-to-encourage-doctors-to-prescribe-health-apps/)

[10] Comstock, Jonah, "NHS England Launches Library for Accredited Mobile Health Apps," March 24, 2015. (http://mobihealthnews.com/41727/englands-nhs-launches-library-for-accredited-mobile-health-apps/)

[11] SEC. 201. [21 U.S.C. 321] - U.S. Food and Drug Administration. (http://www.fda.gov/Regulatory Information/Legislation/FederalFoodDrugandCosmeticA) Accessed April 2, 2015.)

[12] U.S. Food and Drug Administration, "Examples of Mobile Apps for Which the FDA Will Exercise Enforcement Discretion." (http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/ConnectedHealth/MobileMedicalApplications/ucm368744.htm) Accessed April 2, 2015.

[13] PWC Health Research Institute, "Top Issues Consumer Survey," 2014.

[14] PWC Health Research Institute, "Clinician Survey," 2014.

[15] "Global Medical Device Industry Outlook for 2015," Emergo, Published January 2015, http://www.emergogroup.com/resources/research/annual-medical-device-industry-survey

[16] "The Impact of Medical Device Reimbursement on Cost, Innovation and Health Outcomes," (http://files.publicaffairs.geblogs.com/files/2014/08/The-Impact-of-Medical-Device-Reimbursement-on-Cost-Innovation-and-Health-Outcomes.pdf) Accessed April 13, 2015.

[17] Ibid

[18] Beinfeld et al., "Diagnostic Imaging Costs: Are They Driving Up the Costs of Hospital Care?" Radiology. 2005 June; 235(3):934-9.

[19] Taylor, Nick Paul, "European Regulatory Roundup: France Wants More Sunshine for Industry Payments," March 5, 2015. (http://www.raps.org/Regulatory-Focus/News/2015/03/05/21655/European-Regulatory-Roundup-France-Wants-More-Sunshine-for-Industry-Payments-5-March-2015/0)

[20] "Anthem Begins Offering Post-breach Credit Monitoring," February 13, 2015, USA Today, http://www.usatoday.com/story/tech/2015/02/13/anthem-breach-credit-monitoring/23378961/

[21] "Cybersecurity in Medical Devices: Paranoia, or a Tangible Threat?" January 23, 2015. (http://healthworkscollective.com/nishita-pereira-gracias/288481/cybersecurity-medical-devices-paranoia-or-tangible-threat)

[22] "The FDA Takes Steps to Strengthen Cybersecurity of Medical Devices." (http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm416809.htm) Accessed April 20, 2015.

[23] "Dick Cheney Feared Terrorists Could Shock His Heart: Gets Wireless Disabled," (http://www.examiner.com/article/dick-cheney-feared-terrorist-could-shock-his-heart-gets-wireless-disabled) Accessed April 20, 2015.

[24] Alexander, William, "Baranaby Jack Could Hack Your Pacemaker and Make Your Heart Explode," June 25, 2013. (http://www.vice.com/read/i-worked-out-how-to-remotely-weaponise-a-pacemaker) Accessed April 15, 2015.

[25] Appleby, Julie and Hernandez, Daniela, "Can Hackers Get Into Your Pacemaker?" The Atlantic, November 20, 2014. (http://www.theatlantic.com/health/archive/2014/11/can-hackers-get-into-your-pacemaker/382893/) Accessed April 2, 2014.

[26] "Anthem Begins Offering Post-Breach Credit Monitoring," February 13, 2015, USA Today, http://www.usatoday.com/story/tech/2015/02/13/anthem-breach-credit-monitoring/23378961/

[27] PWC Health Research Institute, "Top Issues Consumer Survey," 2014.

[28] http://selectusa.commerce.gov/industry-snapshots/medical-device-industry-united-states. Accessed March 31, 2015.

[29] Shah, Shahid, "Cybersecurity as A Competitive Differentiator for Medical Devices," Med Device Online, March 24, 2015. (http://www.meddeviceonline.com/doc/cybersecurity-as-a-competitive-differentiator-for-medical-devices-0001)

[30] "Ethical Failure Leaves One Quarter of All Clinical Trials Unpublished, October 29, 2013. (http://blogs.nature.com/news/2013/10/ethical-failure-leaves-one-quarter-of-all-clinical-trials-unpublished.html)

[31] Ibid

[32] Flemying, Ella and Shanahan, Daniel, "Overcoming Publication Bias In Clinical Trials," March 17, 2015. (http://www.alltrials.net/news/overcoming-publication-bias-in-clinical-trials-jnrbm-article-collection/)

[33] Peart, Karen N., "Yale YODA Project Announces First Availability of Medical Device Trial Data," Yale News, January 14, 2015. (http://news.yale.edu/2015/01/14/yale-yoda-project-announces-first-availability-medical-device-trial-data)

[34] Kass-Hout, Taha A.,"OpenFDA: Innovative Initiative Opens Door to Wealth of FDA's Publicly Available Data," FDA Voice, June 2, 2014. (http://blogs.fda.gov/fdavoice/index.php/2014/06/openfda-innovative-initiative-opens-door-to-wealth-of-fdas-publicly-available-data/)

[35] Campbell, D. Jeffrey and Sharkey, Brian P.,"Do Start Believin': The Life Sciences Industry's Journey to Global Transparency," August 2014. (http://www.pbnlaw.com/media/510344/Do-Start-Believin-White-Paper.pdf)

Related Videos


Becoming More Competitive with MasterControl


Benefits of MasterControl to Senior Management


Creating a Paperless Process Using MasterControl

About MasterControl Inc.

MasterControl produces software solutions that enable regulated companies to get their products to market faster, while reducing overall costs and increasing internal efficiency. MasterControl securely manages a company's critical information throughout the entire product lifecycle. Our software is known for being easy to implement, easy to validate, and easy to use. MasterControl solutions include quality management, document management, product lifecycle management, audit management, training management, document control, bill of materials, supplier management, submissions management, and more. Supported by a comprehensive array of services based on industry best practices, MasterControl provides our customers with a complete information management solution across the enterprise. For more information about MasterControl, visit www.mastercontrol.com or call 1.800.825.9117 (U.S.); +44 (0) 1256 325 949 (Europe); or +81 (03) 5422 6665 (Japan).

WPXXXXUSENLT-04/15

MasterControl

Corporate Headquarters:
MasterControl Inc.
Salt Lake City, UT
United States
Phone: 1 866 747 8767

European Headquarters:
MasterControl Global Limited
Basingstoke
United Kingdom
Phone: +44 (0) 1256 325 949

Asian Headquarters:
MasterControl KK
Tokyo
Japan
Phone: +81 (3) 5422 6665

Contact information and addresses for other regional MasterControl offices and MasterControl partner offices are listed on the MasterControl website at www.mastercontrol.com.