This publication is part of the Deloitte Center for Regulatory Strategy, Americas cross-industry series on the year’s top regulatory trends. This annual series provides a forward look at some of the regulatory issues we anticipate will have a significant impact on the market and our clients’ businesses in 2019. The issues outlined in each of the reports provide a starting point for an important dialogue about future regulatory challenges and opportunities to help executives stay ahead of evolving requirements and trends. For 2019, we provide our regulatory perspectives on the following industries and sectors: banking; capital markets; insurance; investment management; energy, resources, & industrials; life sciences; and health care.

We hope you find this document to be helpful as you plan for 2019 and the regulatory changes it may bring. Please feel free to contact us with questions and feedback at CenterRegulatoryStrategyAmericas@deloitte.com.
Contents

Introduction 2
Drug pricing 3
Cybersecurity for medical devices 5
MDR regulation 8
Interactions with health care providers 9
Transparency 10
Combination products 12
Market access 15
Taking the lead in times of change 18
Endnotes 20
Contacts 21
Introduction

Life sciences companies exist to help patients and save lives. Regulatory compliance provides guardrails to ensure all companies play by the same rules; however, the overall mission to serve the public and make the world a better place remains constant regardless of shifts in the regulatory landscape.

Compliance modernization helps companies pursue their core mission and achieve compliance as efficiently and effectively as possible by “thinking forward” and then harnessing the best available compliance practices and technologies to comply with current and future regulatory requirements. This is an ongoing need driven by never-ending technological advances and market expectations that are constantly rising.

In life sciences, we expect modernization to be a common theme across all of the key regulatory trends for 2019:

- Drug pricing
- Cybersecurity for medical devices
- MDR regulation
- Interactions with health care providers
- Transparency
- Combination products
- Market access

All of these areas present significant opportunities for improved efficiency and effectiveness, especially with breakthrough technologies such as robotic process automation, advanced analytics, artificial intelligence, and integrated governance, risk, and compliance (GRC) platforms redefining the boundaries of what is possible. We highlight opportunities to modernize compliance in several of our topics, including interactions with health care providers and transparency. It is important to know that regardless of the regulatory issue at hand, there is an opportunity to modernize the compliance operations to support the most efficient and effective path forward for your organization to mitigate the risks associated with that issue.

No matter how “modern” a company’s existing compliance systems and processes might be, there is always room to improve. And ironically, the best time to pursue compliance modernization is when there is less buzz about new regulations and current requirements are leveling off or scaling back—because you actually have the time and resources to focus on it in a thoughtful way, instead of scrambling just to stay in compliance. Looking ahead, compliance modernization is likely to receive significant attention from life sciences companies in 2019.
Drug pricing is a hot topic receiving significant attention from regulators, media, and the general public. Here are a number of key trends and developments:

340B Drug Pricing Program compliance
The 340B Drug Pricing Program appears to be entering a period of significant change, with the pending Final Rule and the Office of Pharmacy Affairs Information System (OPAIS) ceiling price reporting system creating an environment of uncertainty for the life sciences industry. Manufacturers should closely monitor 340B program developments and prepare to respond promptly and effectively to changes in legal requirements. This may require focusing additional resources on 340B program compliance.

The Ceiling Price and Manufacturer Civil Monetary Penalties Regulation (Final Rule) goes into effect on January 1, 2019. According to the Health Resources and Services Administration (HRSA), the system for manufacturers to report ceiling prices will not be available until after the Final Rule takes effect. Revisions to the regulation are still possible, as are Congressional actions. The result could be further changes to manufacturer compliance obligations for 340B.

With the Final Rule taking effect at the beginning of 2019, manufacturers might want to consider moving forward with adopting some of its provisions, including:

- **Medicaid Drug Rebates Program (MDRP) restatements.** A requirement for manufacturers to restate 340B ceiling prices and issue refunds to covered entities within a defined timeframe (i.e., in the case of Average Manufacturer Price [AMP] or Best Price [BP] restatements for errors, and in the case of BP true-ups for late-arriving data).
- **True-up of estimated ceiling prices.** A requirement for manufacturers to true-up estimated ceiling prices for new drugs and then issue refunds to covered entities within a defined timeframe.
- **Offsetting/de minimis threshold.** A prohibition against offsetting overcharges with undercharges to 340B covered entities, and against applying a de minimis threshold to refunds (absent consent from the covered entity that is due a refund).

Manufacturers should consider planning now for the forthcoming changes, since it is never clear how much lead time they will be given to achieve compliance once a new requirement is announced or becomes effective. With an effective date now set at the beginning of 2019, manufacturers should work toward establishing new restatement and refund processes as soon as possible.

**State price transparency reporting**
A growing number of US states have passed—or are in the process of passing—new regulations designed to limit drug costs by requiring reporting on drug prices and drug price increases. This legislative push has largely been a response to the industry trend of increasing Wholesale Acquisition Cost (WAC) prices, and the inability of drug pricing legislation to be passed at the federal level.

These changes further complicate the regulatory landscape and increase pricing pressures, leading to a need for greater transparency and additional reporting capabilities. State-level price transparency reporting legislation, including what is made public or considered proprietary, is generally not consistent across states, and will thus require careful analysis of each requirement to understand the intricacies and reasonable assumptions necessary for compliant reporting.

How can manufacturers respond?
- **Tracking and assessment.** Many manufacturers have started tracking and reviewing both pending and enacted legislation to understand the new requirements.
- **Reporting.** Manufacturers who have triggered reporting requirements have begun reporting to the appropriate states.
- **Cross-functional considerations.** Manufacturers realize that a diverse set of skills and knowledge are required to comply with state price transparency reporting, and many are starting to organize cross-functional workgroups to evaluate enacted and pending legislation.
- **Documentation.** To comply with new state requirements, manufacturers will likely need to develop standard operating procedures or work instructions to comply with new reporting.
- **Reasonable assumptions.** In cases where state legislation is not specific about the timing or manner of reporting, manufacturers have begun to develop reasonable assumptions to guide their compliance activities.
- **Pricing strategy design.** Many manufacturers have also started to analyze the new legislation’s impact on future business decisions—and the potential need to reevaluate their pricing strategies.

Manufacturers should address the complexities that could result from reported prices being available to the public, including competitive challenges, public relations issues, and the potential for information to be misinterpreted. These types of challenges must be understood in order to respond to the regulations and act in a compliant manner.
Trump administration’s blueprint and its policy proposals to lower drug prices
On May 11, 2018, President Trump released the American Patients First Trump Administration Blueprint to Lower Drug Prices and Reduce Out-of-Pocket Costs. The blueprint describes four key challenges confronting the American drug market:

• Higher list prices for drugs
• Medicare beneficiaries and government programs paying higher prices for drugs due to lack of the latest negotiation tools
• High and rising out-of-pocket costs for consumers
• Foreign governments setting lower prices for products developed by American companies

Given the challenge of lowering prices without stifling innovation, the blueprint lays out four strategic principles for drug pricing reform: Improved competition, better negotiation, incentives for lower list prices, and lowering out-of-pocket costs. Together, these principles underpin a move to rationalize pricing through greater transparency for consumers, more negotiating leverage for purchasers, and the elimination of legal obstacles that have slowed the introduction of generic competition.

Beyond its statement of principles, the blueprint laid out a number of concrete policy proposals. Actions both before and since its release show that federal officials continue to maintain a serious focus on bringing down the costs of prescription drugs while supporting drug manufacturers’ ongoing work on new treatments.

Value-based contracts
On June 27, 2018, CMS approved a Medicaid State Plan Amendment (SPA) allowing Oklahoma to negotiate with drug manufacturers for supplemental rebates under value-based purchasing agreements. Although other states have won approval for Supplemental Rebate Agreements (SRAs), Oklahoma’s SPA is the first that specifically provides for additional rebates to be made to the state if a prescription drug falls short of negotiated clinical benchmarks.

Products covered under an SRA with Oklahoma will have preferred status on the state’s Medicaid formulary and may be placed on lower tiers of the state’s drug listings, granting exemptions to utilization management policies such as prior authorization. The updated agreement applies to drugs dispensed effective January 1, 2019.

Under the MDRP, state Medicaid programs receive a minimum rebate of 23.1 percent off the AMP, or if the price is lower, manufacturers must grant Medicaid programs rebates amounting to the BP offered to any other purchaser.

The blueprint asks whether the “best price” standard can cause drug manufacturers to inflate prices for certain products with a high proportion of Medicaid sales. Existing statutes may permit CMS to rewrite regulation so that BP is instead calculated based on actual sales and the observed value of the drug to a patient’s health. Such a change could encourage competition and introduce a new dynamic of value-based contracts to the Medicaid pharmaceutical market.
Cybersecurity for medical devices

United States regulatory outlook

Food and Drug Association (FDA) Pre-Cert program—Software as a Medical Device

The International Medical Device Regulators Forum (IMDRF), of which the FDA is a member, defines “Software as a Medical Device” (SaMD) as software intended to be used for one or more medical purposes that perform these purposes without being part of a hardware medical device. SaMD may be used in combination with other products, including medical devices, and may interface with other medical devices, including hardware medical devices and other SaMD software, as well as general purpose software.

The FDA has established a Software Precertification (Pre-Cert) Pilot Program to provide guidance related to the development of a regulatory model for assessing the safety and effectiveness of software technologies without inhibiting patient access to these technologies. The goal of the program is to streamline “regulatory oversight of software-based medical devices developed by manufacturers who have demonstrated a robust culture of quality and organizational excellence, and who are committed to monitoring real-world performance of their products once they reach the US market.” In practice, this could potentially translate into faster review and clearance to market of regulatory submissions for SaMD offerings.

The latest version of the working model (v0.2) for the development of software under the Pre-Cert Pilot Program was publicly released in June 2018 and provides an overview of the program and its operating components. The program allows for precertification of software manufacturers who meet the requirements and would leverage data from all appropriate sources. Within the Pre-Cert Pilot Program, the FDA evaluates an organization against five culture-of-quality and organizational excellence (CQOE) principles (i.e., “excellence principles”): Product Quality, Patient Safety, Clinical Responsibility, Cybersecurity Responsibility, and Proactive Culture.

The FDA is working with a number of technology and medical device companies to create the pilot program, and hopes to launch it sometime in 2019. Once launched, the program will continue to mature based on lessons learned from pilot program participants—improvements that can then be applied to the program, regulation, and leading industry practices.

FDA Safety Action Plan

On April 18, 2018, the FDA released the latest version of its Medical Device Safety Action Plan: Protecting Patients, Promoting Public Health, which aims to improve patient safety, explore regulatory solutions, and advance medical device cybersecurity nationwide. The plan provides additional insight into the agency’s plans beyond its already-published guidance, which includes: Content of Premarket Submissions for Management of Cybersecurity in Medical Devices, and Postmarket Management of Cybersecurity in Medical Devices.

Within the Medical Device Safety Action Plan, the FDA is considering updates to its existing premarket cybersecurity guidance. Medical devices will need the ability to update and receive security patches. Also, a software bill-of-materials (SBOM) will need to be provided to the FDA as part of a premarket submission and made available to medical device customers and users. In addition, the FDA plans to update the premarket guidance on medical device cybersecurity to better protect against moderate risks (e.g., ransomware campaigns) and major risks (e.g., remote, multipatient catastrophic attacks).

From a postmarket perspective, the FDA is considering a new postmarket authority to require that firms adopt policies and procedures for coordinated disclosure of vulnerabilities as they are identified. In addition, the FDA is exploring the development of a CyberMed Safety (Expert) Analysis Board (CVMASB). This board’s responsibilities might include assessing vulnerabilities, evaluating patient safety risks, adjudicating disputes, assessing proposed mitigations, providing consulting to organizations navigating the coordinated disclosure process, and serving as a “go-team” that could be deployed in the field to investigate a suspected or confirmed device compromise at the request of the manufacturer or FDA.

As a result of the plan, stakeholders (e.g., customers, device manufacturers, health care delivery organizations) should start preparing for these additional design considerations and processes, taking the appropriate steps to secure their connected medical devices throughout the life cycle and reduce risk to patient safety and information security.

FDA proposes modernization of medical device approval pathway

A new proposal to modernize the 510(k) clearance pathway would impact nearly 80 percent of medical devices that undergo review by the FDA. The FDA proposal aims to ensure that devices in the approval pathway account for modern technology advancements and are based on modern safety and performance criteria.
As new devices incorporate more sophisticated technologies, such as automation and robotics, FDA plans to bring changes to what companies consider predicate devices. Currently, as lower-risk devices seek FDA approval through the 510(k) pathway, they are compared to devices that have been on the market for decades.

Under the proposal, the FDA is considering a specification that would require applications to compare devices with products that have been on the market for less than 10 years. Additionally, the agency is working on an alternate “Safety and Performance Based Pathway” for categorically well-understood devices that would rely on objective criteria absent of a predicate device.

International regulatory outlook

China FDA regulation

With China’s continued focus on improving its technological competence, the Chinese government has enacted a series of laws, regulations, and standards intended to increase the country’s cybersecurity. One of these laws is the Cybersecurity Law (CSL), which aims to (1) provide the foundation for future laws on cybersecurity; (2) normalize Chinese domestic data management and internet usage regulations; and (3) impose new requirements for network and system security. In accordance with the implementation of the CSL, the China Food and Drug Administration (CFDA) issued its Guiding Principles on the Technical Reviews of Cybersecurity Registration of Medical Devices (Guiding Principles), which went into effect on January 1, 2018.

The basic principle that has served as the impetus for China’s focus on medical device cybersecurity is as follows: “With the advent of interconnected medical devices, we have seen an increase in the quality of medical services provided to patients. Yet, in contrast, we have also seen firsthand the susceptibility to exploitation this elevated interconnectivity brings.” This potential for exploitation underscores the necessity for cybersecurity considerations within medical devices to help mitigate the risks related to patient privacy and unintended operation of the device.

Although the Guiding Principles are not mandatory, the CFDA suggests that manufacturers perform a self-assessment of the relevant cybersecurity protection measures based upon international standards such as the IEC/TR 80001-2-2:2012 “Application of risk management for IT-networks incorporating medical devices.” Failure to meet the requirements could lead to delays with product registrations, exposure to potential penalties under CSL, and negative impacts on a product’s success.

Medical device manufacturers looking to sell their devices in China need to establish processes that align with the CFDA’s Guiding Principles. For successful registration, manufacturers should include technical details in the following three areas: Software Research Documentation (Cybersecurity Description File), Product Technical Requirements, and Instructions for Use. In addition to these technical considerations, which are primarily premarket, manufacturers should also consider cybersecurity issues that may arise once the device is in the field (i.e., postmarket) and they will need to submit a formal “Change Registration” if there is a change to the medical device that may have cybersecurity implications.
European Union (EU) General Data Protection Regulation (GDPR)
The EU’s General Data Protection Regulation (GDPR) is a stringent regulation related to data protection and privacy specifically for EU residents. While the scope of GDPR specifically pertains to EU residents, in practice it is borderless and sector-neutral because it applies to any organization, even those based outside of the EU, that: (1) collects data on EU residents (i.e., a “data controller”); (2) processes data on behalf of a data controller (i.e., a “data processor”); (3) offers goods or services to customers in the EU; (4) monitors the (online) behavior of EU customers; and/or (5) processes, hosts, or stores the personal data of EU customers.

One significant change introduced by the GDPR is a broader definition of personal data, which now includes information about factors specific to an individual’s physical, physiological, genetic, mental, economic, cultural, or social identity. It also explicitly includes location data, IP addresses, and online/technology identifiers.

GDPR has a number of requirements that are driving impacted organizations (e.g., medical device manufacturers, health care delivery organizations) to make significant changes. Of these changes, organizations are likely struggling the most with (1) understanding what data they have and where they reside; (2) implementing privacy-by-design; and (3) complying with data breach reporting requirements. Contributing to these challenges is the need to secure both traditional IT systems and medical devices that may be creating, storing, using, and transmitting data of EU patients and customers. Implementing security-by-design and privacy-by-design for medical devices is a particularly unique and difficult challenge for the industry.

One of the GDPR’s largest impacts is its potential penalties for noncompliance: up to 4 percent of annual global turnover or 20 million euros, whichever is greater. The GDPR’s new requirements and enforcement considerations, combined with increasing demands from consumers, have pushed privacy and security to the top of the corporate agenda and led many organizations to strengthen their privacy and security teams and capabilities.
After approval by the European Parliament, the EU Medical Device Regulations (MDR) (2017/745) and In Vitro Diagnostic Regulations (IVDR) (2017/746) both went into effect in May 2017. The clock is now ticking on a three-year implementation window for the MDR and a five-year window for the IVDR.

Compliance with the MDR is more than just a paper exercise to revise some procedures. Substantive changes are required that can significantly affect an organization’s regulatory profile, product portfolio, and market share. Changes include:

- Reclassification to a higher risk category for some devices, requiring more complicated and extensive regulatory submissions
- More stringent requirements around clinical data, with stronger clinical evidence needed to support regulatory submissions both pre- and postmarket
- More expansive postmarket requirements for adverse event monitoring and reporting

Some manufacturers may see these enhanced regulations as potentially leading to a number of long-term issues, including:

- Longer time-to-market for new products
- Higher costs to bring products to market and maintain their position in the market
- Possible talent shortages, and challenges in identifying and retaining qualified personnel
- Potential challenges in working with Notified Bodies, who themselves may have staffing issues and increased regulatory surveillance requirements
- A need to assess product portfolios and eliminate some products for which the cost/benefit ratio under the new regulations cannot be justified

Many organizations are struggling to understand the impact of these changes, especially as information from regulators and Notified Bodies has been limited to date. In addition, these new regulations are not being implemented in a vacuum. Other changes, such as the new ISO 13485:2016 “Medical devices—Quality management systems—Requirements for regulatory purposes” and the Medical Device Single Audit Program (MDSAP), both of which are being implemented concurrent with the MDR and IVDR, require significant changes to an organization’s Quality Management System. All of this is in addition to the changes required for submissions and reporting under the MDR.

Medical technology companies that wish to continue to operate in the EU under these new regulations must have a clear plan in place, the proper resources to implement the plan, and a commitment from leadership to make the tough decisions and choices that will be needed to achieve continued compliance.
Interactions with health care providers

Pharmaceutical, biotech, and medical device companies routinely interact with external health care providers, either through contractual arrangements (e.g., fee for service) or noncontractual arrangements (e.g., providing lunches to doctors’ offices). These health care provider (HCP) interactions have been scrutinized by regulators, legislators, and the media for the better part of two decades, and will likely continue to receive close scrutiny for the foreseeable future.

The risks for life sciences companies in this critical area stem from potential violations of laws (e.g., Anti-Kickback Statute) and regulations (e.g., Physician Payments Sunshine Act), and from the prospect of negative media attention.

This issue is not new, and is not going away anytime soon. External HCP relationships will likely remain under the watchful eye of lawmakers, regulators, and the media for years to come, which makes it essential for companies to manage and execute these arrangements as efficiently and effectively as possible, with appropriate controls and documentation.

In addition to having the right policies and procedures in place, which is essential, today’s life sciences companies also should consider leveraging technology solutions to automate activities and controls—and to assist with ongoing compliance monitoring. The processes required to create an efficient yet effective control environment for managing HCP relationships are numerous, repetitive, and sometimes complex. Relying on human resources alone, or with only minimal support of technology solutions, exposes a company to unnecessary risk and limits its efficiency.

Until recently, many companies were slow to make technology investments in this area. However, with major advances in automation and artificial intelligence, a growing number of life sciences companies are taking the long-term view and investing in solutions and tools that can significantly improve their ability to manage HCP interactions in an efficient and compliant manner.

One compelling use case for these powerful new technologies is workflow automation. Today, many companies still manage HCP interactions using an archaic system of spreadsheets, email, and manual processing. This is labor-intensive, time-consuming, and prone to errors. The good news is companies now have ready access to a variety of cloud-based applications and other automation tools that can significantly improve efficiency, speed, and consistency. For example, a cloud-based fair market value (FMV) calculator provides a single definitive source for instantly determining the fair market value of a particular HCP and activity type, eliminating the need to manually wade through and reconcile a jumble of spreadsheets. The calculator also automates the exception process, triggering follow-up emails as needed and managing the entire approval process without the need for human coordination. Just as important, all of the decisions and actions that go into determining the final FMV are consistently and objectively applied, with automatic documentation and archiving for easier defense in an audit.

A second use case that is even more sophisticated and compelling takes automation to the next level by harnessing the power of cognitive technologies. For example, it is now possible to create an automated process for reviewing and approving HCP contracts with little or no human involvement. Natural language processing analyzes terms and conditions; software bots apply rules and artificial intelligence to evaluate contracts and qualifications using the same criteria as humans, replacing or augmenting human judgment; and machine learning enables the system to learn from experience and get smarter over time. Already, these intelligent systems can accurately and confidently make “approve?”“reject” decisions for more than 70 percent of contracts—and in the minority of cases where the system is unsure, it automatically routes the contract to a human expert with questionable elements highlighted to make the manual decision-making process much faster and easier.

A third use case combines cognitive technologies with data analytics, using cluster analysis to find hidden patterns in large data sets. For HCP interactions, one way this technology could be used is for identifying high-risk HCPs and potential compliance violations where the volume of payments or interactions with a particular HCP is approaching regulatory limits.

By investing in automation and cognitive technology solutions, a life sciences company can significantly improve their efficiency and effectiveness in managing HCP interactions, while at the same time reducing their risk exposure. What’s more, those same technologies and solutions can be tailored to address a wide range of business processes, not just those involving HCP interactions—enabling companies to enhance their benefits and ROI by leveraging their investments across the entire enterprise.
Over the past few years, the federal government has been actively increasing its use of Open Payment information to cross-reference HCP engagement activities with data from other organizations to monitor compliance. As stated by Centers for Medicare & Medicaid Services (CMS), the Open Payments Sunshine data are shared with other agencies when disclosure is deemed “reasonably necessary by CMS to prevent, deter, discover, detect, investigate, examine, prosecute, sue with respect to, defend against, correct, remedy, or otherwise combat fraud, waste or abuse in such programs.”16 Combined with other data publications (such as Medicare Part D and Part B), regulators now have ever-increasing opportunities and avenues for investigative inquiries of drug and device companies.

Given the vast transparency through the data and analytics tools that federal regulators now have at their disposal—along with regulators’ stated intent to use those resources for compliance and enforcement—it is prudent for life sciences manufacturers to consider developing their own advanced capabilities in these areas. This can enable companies to proactively identify and mitigate potential compliance problems before regulators take formal action—an approach that regulators don’t just encourage but expect.

Companies are expected to be proactive on transparency analytics and compliance

In her keynote address at the 2015 Pharmaceutical Compliance Congress, US Department of Health and Human Services (HHS)—Office of Inspector General (OIG)—Senior Counsel Mary Riordan stated: “Companies have spent a lot of time, effort, and resources to comply with open payments reporting requirements, and I would recommend that [they] capitalize on those investments.”17

In 2016, the US Department of Justice (DOJ) expressed a similar sentiment. “I think there are a lot of things that companies can do with that information, with the data they’ve been collecting, to identify problem areas and to address them,” said Laura M. Kidd Cordova, Assistant Chief, Criminal Division, Fraud Section, DOJ. She further noted that “when we get to the point that we’re charging anybody or even proceeding in an extensive investigation, there’s other evidence that we’ve collected. And so I think it’d be a good idea for the companies to basically go through the same steps.”18

What’s more, federal regulators are not the only interested parties comparing and analyzing data across data sets; the press and industry watchdog groups are also cross-referencing Open Payments data with available Medicare Part D data to identify and publish payment trends, identify prescribing patterns, and draw conclusions. Given today’s data-driven business environment—with its unprecedented volume and accessibility of internal and third-party data—life sciences companies should view the Open Payments system as a valuable tool in their ongoing compliance efforts. Over the past two years, government regulators, OIG, and DOJ have openly stated that they will combine Open Payments data with other available data sets to pursue anti-kickback investigations. As the accuracy of data submitted to CMS and data maintained internally in source systems increases, regulators expect manufacturers to fully utilize those data sets to support proactive compliance efforts. At a minimum, life sciences manufacturers should be able to correlate supporting data and/or supporting documents to help (1) detect compliance patterns and take corrective actions before they become issues, (2) explain any identified anomalies, and (3) use these findings to enhance compliance and HCP engagement programs.

Specifics to focus on

Although vendors generally offer basic analytics modules for their transparency reporting systems, the industry trend is for companies to maintain their own, more sophisticated data repositories and analytics capabilities that combine transparency reporting data with other internal and external data sources—enabling insights that are more powerful and valuable, both from a compliance and commercial perspective.

Specific areas to focus on when considering more advanced transparency analytics capabilities include:

Data cleansing. Now that transparency reporting is a routine practice, most companies have implemented procedures to address and maintain the quality of their transparency data. However, data quality is a never-ending challenge that requires constant vigilance. Also, as companies expand the scope of their transparency analytics to include other data sources, the same level of quality and rigor needs to be applied to those additional data sets.

Infrastructure. Given the industry-wide reliance on third-party, cloud-based solutions for transparency reporting (and most other IT systems), many manufacturers may not have the infrastructure and expertise necessary to develop and operate their own custom IT solutions for transparency analytics. Among other requirements, companies will
Leading in times of change
Life sciences regulatory outlook 2019

need processes, policies, and procedures to ensure the right transparency data are transferred from an outside vendor’s systems at the right time—and that they are combined and maintained with data from other sources in a reliable and robust way. Also, companies will need clear and effective policies to make sure that commercial-focused analytics do not violate compliance restrictions on use of spend data for commercial/marketing analytics.

Cross-functional teams. Effective transparency analytics require involvement from many areas of the business, not just IT. The cross-functional team, and their collective requirements, should drive the implementation of these analytics. Also, as more and more jurisdictions around the world impose their own requirements for HCP transparency and data privacy, the transparency analytics effort can quickly become a global challenge that requires involvement and input from the entire global enterprise. At the same time, it can create a valuable opportunity to catalyze global harmonization of transparency-related processes and policies.

Getting started
The most common mistake when getting started with transparency analytics is focusing on technology solutions first, and then working backwards to make the business process or analysis needs fit the selected/implemented technology. Another approach is to start by carefully considering the information needs of your business—who are all the relevant stakeholders and what do they want to know? What are competitors leveraging these data for? How is success of the initiative measured? It is also important to consider how your business is organized, and what kind of operating model for transparency analytics makes the most sense: Centralized or decentralized? Global or country-specific? In-house or outsourced? Once you understand the business issues or requirements, it is much easier to determine which tools and algorithms are the best fit.
Combination products are revolutionizing pharmaceuticals, biotechnology products, and medical devices (henceforth referred to as “life sciences products”) and transforming the patient experience—simplifying delivery methods, providing controlled release of medicine, and improving patient adherence. However, the rise of combination products is also creating a more complex regulatory landscape.

The FDA classifies combination products as “therapeutic and diagnostic products that combine drugs, devices, and/or biological products.” Examples include insulin injectors, light-activated drugs, first aid kits, and artificial replacement organs such as the bio-artificial pancreas. The regulatory landscape for such products is complex and complicated, with agency regulations and expectations evolving globally at different speeds (see figure 1). In 2013, the FDA released the Final Rule 21CFR Part 4 cGMP Requirement for Combination Products, and in 2016 it released the Postmarketing Safety Reporting Final Rule, with enforcement planned to start July 2019. By contrast, the European Medicines Agency (EMA) has only recently passed a provision to recognize combination products (known in the EU as drug-device combination products [DDCs]) and regulate them under a separate rule—the EU Medical Device Regulation Compliance rule, which was published in 2017 and has a compliance date of May 2020.

In addition to challenges created by the evolving regulatory landscape, regulation of combination products is particularly complicated because the products contain components traditionally monitored by...
different departments within the regulatory authorities. Variations in protocol for each of the regulatory bodies can make it hard for a product to move efficiently through the regulatory process.

Another complication is that some well-established companies wound up in the market for combination products without a deliberate intent or strategy—it was simply a natural evolution of their traditional standalone products, or combination product portfolios were acquired through merger and acquisitions. As such, they might not have the necessary skill sets in place, and even now might not fully realize they are in the combination products business.

Given these challenges, many life sciences companies are struggling to comply with the emerging regulations. In particular, a number of companies have received warning letters from the FDA citing a failure to comply with good manufacturing practices and quality management system defects for combination products.

To address the changing regulatory landscape and avoid compliance violations, companies should review the latest updated quality management regulatory requirements for combination products, and then see how their product offerings and business practices stack up.

A leading practice is to implement a five-pronged holistic approach so companies can make sure they are prepared to achieve and maintain compliance while expanding their combination product portfolios.

The first step for companies, whether or not they are expanding their combination product offerings, is to conduct a thorough

---

**Research and development**

Combination products, with their diverse components, are a great example of the need for improved integration and coordination of Research & Development (R&D) compliance activities across all life sciences functions—Clinical, Regulatory, Safety, and Medical Affairs—as well as Strategy and Technology, which are foundational capabilities that span individual functions. However, in today’s increasingly complex regulatory environment for medical devices and life sciences products, improved integration and coordination are important for all R&D compliance efforts—including those that focus solely on traditional product offerings, which are narrower in scope.

Based on our experience working with leading life sciences companies around the world, here are four key enablers that can help improve integration and coordination in R&D compliance:

- **Unified regulatory information management (RIM).** Strategic, efficiently integrated RIM capabilities and systems—including content management, publishing, submission, archiving, etc.—can help drive efficient and accurate, end-to-end regulatory processes and greater consistency.

- **Global regulatory intelligence.** Regulatory requirements vary widely around the world and are constantly changing. Global intelligence capabilities track and capture all of those diverse requirements in a single global database that is definitive, comprehensive, searchable, and continuously updated. This capability can drive several downstream effects such as faster time to market and increased level of compliance.

- **Optimized labeling.** Creating, maintaining, and updating all of the detailed label information that must be dispensed with medical devices and life sciences products—leveraging experience in regulatory operating model design, process improvements, automation, and technology implementation.

- **Faster filing.** Enhancing the flow of information among key functions—Regulatory, Supply Chain, and Manufacturing—by streamlining processes, technologies, and solution providers can help achieve new levels of speed and compliance.
review of their current products to make sure all combination products are identified and classified appropriately.

The second step is to thoroughly review all current and upcoming regulatory requirements globally, and then conduct a readiness assessment to see how well the business is positioned to comply—and to identify any gaps in processes or roles that may require adjustment. Also, a process should be established to continually monitor combination product regulations around the world, with a particular focus on US and EU regulations, since they already exist.

The third step is to establish effective controls for management, purchasing, and design. Activities around management controls should focus on defining governance structures, strategies, roles, and responsibilities in manufacturing sites. This includes reviewing strategies and procedures for selecting authorized representatives and notified bodies, as well as standardizing plans for manuals and supplemental documentation. Activities around purchasing controls should focus on the criteria for selecting third parties and suppliers globally for internal and external manufacturing. Activities around design controls should focus on identifying whether all processes and capabilities meet regulatory requirements.

The fourth step is to enhance the Corrective Action and Preventative Action (CAPA) plan and the postmarket surveillance plan to identify, define, implement, and monitor processes and capabilities to meet combination product requirements. Activities should focus on improving data analytics, highlighting and monitoring trends, and improving the intake, handling, and investigation processes related to combination product CAPAs.

The fifth step, in line with enhancing CAPA and postmarket surveillance plans, is to conduct a safety review, and then update processes to satisfy the requirements for combination products. Training, reporting databases, third-party surveillance agreements, reporting scopes, and clinical evaluations should all be reviewed and enhanced for adverse events. Also, a thorough review of all current US and EU regulations should be conducted from a safety perspective, updating guidance as needed to highlight leading practices.

As combination products continue to be developed and are becoming more prevalent, companies need to enhance their systems and controls to remain compliant.
Market access

Market access programs are driven by the strategic need to provide patients with access to lifesaving drugs—removing barriers wherever possible. Achieving this goal requires engaging third parties to perform reimbursement support, patient services, co-pay/co-insurance support, distribution, and patient out-of-pocket mitigation programs such as patient assistance programs (PAP).

Leaders in the market access function have the daunting task of holistically integrating the multitude of vendors that play a role in easing patient burden and enabling access. One key intermediary is specialty pharmacies, which distribute specialty drugs that are prescribed for complex conditions such as cancer and HIV.

“Specialty” product characteristics that require a specialty pharmacy include:
- High cost
- Need for special handling
- Need for ongoing assessment
- Treatment for rare disease
- Need for monitoring of side effects
- Self-administered injectable
- Office-administered injection/infusion
- Need for patient training

To address these factors, specialty pharmacies offer a broad range of services and capabilities.

On the operations side, specialty pharmacies have specialized supply chains that adhere to rigorous storage, shipping, and handling standards to meet product label shipping requirements, such as temperature control and the timely delivery of products in optimal conditions. They also offer patient assistance (such as helping eligible patients enroll), care coordination (across health care providers), and reimbursement navigation.

On the clinical side, specialty pharmacies are involved in everything from consulting with physicians and patients, to providing disease- and drug-specific care management services, managing patient adherence, collecting and tracking data on clinical outcomes, and managing care for Risk Evaluation and Mitigation Strategies (REMS).

Legislators and regulators are getting involved in this area out of concern that the processes related to market access through specialty pharmacies might not be well controlled, and that some of the activities might put patients at risk or interfere with the practice of medicine.

Overview of legal risks
The arrangements with specialty pharmacies expose patients to risk—specifically, the risk of not getting the right product at the right time under the right conditions. Also, the arrangements give rise to a number of legal and regulatory compliance-related risks. In particular, manufacturers must take steps to avoid kickback risk by ensuring that payments for services provided by specialty pharmacies:
- Do not provide an inducement to prescribe/use a specific product
- Do not provide patients with extensive services or support—or misrepresent services—in any way that could be perceived as steering them toward a manufacturer’s products
- Do not make discounts conditional on specialty pharmacy performance
- Are provided within the context of a written agreement that satisfies the Safe Harbor provisions of the Anti-Kickback Statute (term longer than one year; clearly itemized services based on bona fide need)

There are other types of risk to be managed as well. Patient privacy must be protected. The manufacturer must take steps to ensure only de-identified data are obtained from the specialty pharmacy. Patients must be informed of how their protected health information (PHI) will be used. Also, adverse event (AE) reporting requirements must be satisfied.

Specific activities to consider
When building a compliance program related to specialty pharmacy interactions, there are several key considerations. Chief among them is the need for a governance model that can support the compliance program. Written standards, training and communication, auditing, and monitoring are central aspects of such a governance model—along with identification of the individuals within a company who will own, operate, and continuously improve the compliance program.

Here are some specific considerations related to specialty pharmacy compliance program design, broken out by key steps in specialty pharmacy operations.

Specialty pharmacy program design
- Companies should develop a written business justification (“needs assessment”) to document the legitimate, bona fide business need for specialty pharmacy services and/or defined distribution networks prior to engaging a specialty pharmacy and/or prior to the addition of services to an existing specialty pharmacy relationship. There should also be a documented process for completing the needs assessment, including who...
is required to complete the needs assessment, what activities the needs assessment must cover, and instructions on how to complete and submit a needs assessment for review and approval.

- A company should also create a standard set of defined services considered to be “core” and “enhanced”;

Specialty pharmacy selection
- Companies should have standard criteria to support the qualification and selection of each specialty pharmacy, considering factors such as: specific service offering capabilities (e.g., combination therapy counseling); relevant experience with the manufacturer; and the ability to comply with manufacturer’s compliance requirements.

- These criteria should be evaluated as part of a documented, standard specialty pharmacy due diligence process that includes background checks on the specialty pharmacy (including relevant exclusion and debarment checks); review of the specialty pharmacy’s compliance and training program; and review of the specialty pharmacy’s process for auditing and monitoring internal operations (and the specialty pharmacy’s ability to implement manufacturer-specific business rules).

Specialty pharmacy contracting, activities, and training
- Companies should develop FMV methodologies to value the contract elements for each specialty pharmacy activity and/or data purchases.

- Contracts should detail the activities to be provided, as well as compliance obligations, audit rights, patient privacy rights, and vendor training requirements.

- Contracts should explicitly state that services and discounts are not conditional on any preference/switching/promotional requirements, and that nothing in the agreement is meant to interfere with the independent clinical judgment of the specialty pharmacy.

- Contracts should document any specific requirements related to interactions and data sharing regarding patient transfers to International Conference of Pharmacy and Advanced Pharmaceutical Sciences (ICPAPS).

- Contracts should require standard patient eligibility criteria for patient education/adherence services against a standard set of criteria/considerations (e.g., patient education/adherence services be limited to on-label uses). Contracts should also require controls to help ensure transparency with patients who participate in manufacturer-funded services regarding how their personal information will be used (e.g., if it will be shared with third parties, or used to market other manufacturer or specialty items/services).

- Contracts should spell out training requirements for specialty pharmacy provider staff related to company compliance requirements, including: AE reporting; product safety; product education; activity execution; compliance with relevant laws and regulations (e.g., Health Insurance Portability and Accountability Act of 1996 [HIPAA], Anti-Kickback Statute); and appropriate/inappropriate interactions and communications between manufacturer sales representatives and specialty pharmacy representatives (e.g., limits on sharing information about the other party’s products or services, and prohibition of sharing patient-specific information about the status of fulfillment of prescriptions at the pharmacy or with a payer).

Specialty pharmacy data collection and use
- Companies should have standards related to the following:
  - What data are collected from specialty pharmacies
  - How data are collected and disseminated, and how data are stored (e.g., where, and for how long)
  - What data the manufacturer is prohibited from receiving (e.g., PHI)
  - Prohibited uses or analyses of specialty pharmacy data (e.g., ROI analysis, or using data to determine size ICPAP financial contributions or free medicine donations)
  - Data security measures to prevent unintended use and access to information
  - Training individuals who might use data about allowable uses of that data (and the related risks)
Specialty pharmacy auditing and monitoring

• Companies should have documented requirements related to the auditing and monitoring of specialty pharmacy activities and data, including requirements that:
  – Auditing/monitoring be completed according to a documented schedule (e.g., an auditing and monitoring plan)
  – Auditing/monitoring results be reviewed with relevant stakeholders
  – A CAPA/remediation plan be developed and documented to address any auditing/monitoring findings
  – The CAPA/remediation plan be reviewed with relevant stakeholders
  – CAPA/remediation progress be tracked and regularly reported to relevant stakeholders

Moving forward
Pharmacy benefit manager-owned specialty pharmacies control 68–80 percent of the market for specialty products; this means that companies seeking to have their products distributed in an efficient and effective manner already face pressure in their specialty pharmacy relationships. Coupled with the current enforcement focus on market access activities generally—and specialty pharmacy activities specifically—as well as the evolving risk landscape and legal issues that go along with it, companies face truly significant challenges in managing risks related to specialty pharmacy relationships. Companies can reduce those risks by taking steps to understand their activities in the space and then further build out the appropriate governance and controls.
Taking the lead in times of change

Today’s regulatory environment is in the midst of significant and unpredictable change, driven by a variety of forces including political shifts, new social norms and behaviors, and technological innovation. To succeed in this challenging environment, companies need to actively look for ways to improve the effectiveness and efficiency of their compliance strategies and operations. Technology is likely to play an increasingly important role in this pursuit. Robotic process automation, for example, is being widely adopted by compliance-related functions to help them do more with less. At the same time, emerging technologies such as artificial intelligence and advanced analytics are making it possible to do things that have never been done before. Innovations like these can create business value no matter which way the regulatory winds might shift—enabling leaders to take action confidently and decisively in times of significant and ongoing change.
Leading in times of change
Life sciences regulatory outlook 2019
Endnotes


10. US Food & Drug Administration, “Statement from FDA Commissioner Scott Gottlieb, M.D. and Jeff Shuren, M.D., Director of the Center for Devices and Radiological Health, on transformative new steps to modernize FDA’s 510(k) program to advance the review of the safety and effectiveness of medical devices,” available at https://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm626572.htm.


14. Ibid.


17. Mary Riordan, OIG Senior Counsel, from her Keynote Address at the 2015 Pharmaceutical Compliance Congress.

18. Laura M. Kidd Cordova, Assistant Chief, Criminal Division, Fraud Section, US Department of Justice, August 16, 2016.


21. Core services are services provided as part of basic specialty pharmacy services, without additional compensation; enhanced services are services that a specialty pharmacy only provides in return for payment.
Contacts

Leadership
Monica O’Reilly  
Regulatory & Operations Risk Leader  
Principal | Deloitte Risk and Financial Advisory  
Deloitte & Touche LLP  
monoreilly@deloitte.com

Dan Ressler  
US Advisory Life Sciences Leader  
Principal | Deloitte Consulting LLP  
dressler@deloitte.com

Paul Silver  
Life Sciences Center for Regulatory Strategy Leader  
Principal | Deloitte Risk and Financial Advisory  
Deloitte & Touche LLP  
psilver@deloitte.com

Authors
Mark DeWyngaert  
Managing Director  
Deloitte Risk and Financial Advisory  
Deloitte & Touche LLP  
mdewyngaert@deloitte.com

Jeff Fisher  
VP, Business Solution Architecture  
Deloitte Risk and Financial Advisory  
Deloitte & Touche LLP  
jefffisher@deloitte.com

Bill Greenrose  
Managing Director  
Deloitte Risk and Financial Advisory  
Deloitte & Touche LLP  
wgreenrose@deloitte.com

Marcy Imada  
Principal  
Deloitte Risk and Financial Advisory  
Deloitte & Touche LLP  
mimada@deloitte.com

Veronica Lim  
Principal  
Deloitte Risk and Financial Advisory  
Deloitte & Touche LLP  
vlim@deloitte.com

Mark Linver  
Managing Director  
Deloitte Risk and Financial Advisory  
Deloitte & Touche LLP  
mlinver@deloitte.com

Oliver Steck  
Principal | Deloitte Risk and Financial Advisory  
Deloitte & Touche LLP  
osticke@deloitte.com

Jack Tanselle  
Managing Director | Deloitte Risk and Financial Advisory  
Deloitte & Touche LLP  
jtanselle@deloitte.com

Mel Walker  
Principal | Deloitte Risk and Financial Advisory  
Deloitte & Touche LLP  
melwalker@deloitte.com

The Center wishes to thank the following Deloitte professionals for their insights, contributions, and support for this report:

Clarissa Crain, Senior Manager, Deloitte Risk and Financial Advisory, Deloitte & Touche LLP  
BJ D’Avella, Senior Manager, Deloitte Risk and Financial Advisory, Deloitte & Touche LLP  
Neil DeHenes, Senior Manager, Deloitte Risk and Financial Advisory, Deloitte & Touche LLP  
Rick Moore, Senior Manager, Deloitte Risk and Financial Advisory, Deloitte & Touche LLP  
Tushar Sangale, Manager, Deloitte Risk and Financial Advisory, Deloitte & Touche LLP  
Nicole Schumacher, Senior Manager, Deloitte Risk and Financial Advisory, Deloitte & Touche LLP  
Nick Sikorski, Manager, Deloitte Risk and Financial Advisory, Deloitte & Touche LLP  
Juan Tessi, Manager, Deloitte Risk and Financial Advisory, Deloitte & Touche LLP  
Clay Willis, Senior Manager, Deloitte Risk and Financial Advisory, Deloitte & Touche LLP
About the Center
The Deloitte Center for Regulatory Strategy provides valuable insight to help organizations in the financial services, health care, life sciences, and energy industries keep abreast of emerging regulatory and compliance requirements, regulatory implementation leading practices, and other regulatory trends.

Home to a team of experienced executives, former regulators, and Deloitte professionals with extensive experience solving complex regulatory issues, the Center exists to bring relevant information and specialized perspectives to our clients through a range of media including thought leadership, research, forums, webcasts, and events.

Deloitte

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

About Deloitte
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States, and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.

Copyright © 2018 Deloitte Development LLC. All rights reserved.