Deloitte.

Navigating the year ahead

2018 life sciences regulatory outlook

United States
December 2017

CENTER *for*
REGULATORY
STRATEGY
AMERICAS

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 2018. 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 2018, we provide our regulatory perspectives on the following industries and sectors: banking, securities, insurance, investment management, energy and resources, life sciences, and health care.

We hope you find this document to be helpful as you plan for 2018 and the regulatory changes it may bring. Please feel free to contact us with questions and feedback at **CenterRegulatoryStrategyAmericas@deloitte.com**.

Contents

Introduction

Most life sciences companies are forging ahead with their risk and compliance initiatives, even as regulatory uncertainty will likely remain a significant and ongoing challenge. Even if lawmakers and regulators make certain definitive changes, life sciences companies must continue to drive the effectiveness and efficiency of their risk and compliance programs so they meet applicable laws, regulations, and supervisory expectations. And in most cases, they don't have the time or luxury of waiting to see how things will shake out. Fortunately, many of the changes life sciences companies are making to achieve compliance are useful improvements that are worth doing from a risk and business perspective.

Here's a look at the key regulatory trends life sciences companies will likely need to monitor and address in 2018. By embracing regulatory complexity, organizations can accelerate performance and stay ahead of changes so they can better navigate the regulatory landscape.

To stay on top of the latest regulatory news, trends, and insights, we invite you to visit our website at www.deloitte.com/us/about-dcrsamericas.

Medical devices: FDA cybersecurity regulatory update

Use of connected medical devices is increasing across the life sciences industry. For medical device manufacturers, top-of-mind issues include improving patient care, extending the remote reach of physicians, and maintaining a competitive advantage. There are many potential benefits associated with connecting medical devices to the internet, hospital networks, mobile products, and other devices or hospital systems. However, achieving those benefits requires effectively addressing the related cyber and patient safety risks.

A growing number of medical device security issues pose a threat to patient safety, product quality, and data integrity. Cybersecurity vulnerabilities in medical devices can be exploited to gain unauthorized access to data on—or transmitted by—devices, networks, and upstream and downstream IT systems. With this access, threat actors can steal patient information, manipulate data, exploit providers, hold information for ransom, alter patient treatment plans, and/or manipulate connected devices to harm the patients that use them.

Taking action to reduce the risks associated with connected medical devices is a growing trend among leaders and regulators in life sciences. The FDA has issued pre- and post-market guidelines to help secure connected medical devices throughout their life cycle and across stakeholders. On June 14, 2013, the FDA issued initial premarket guidance titled "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices."[1] In this document, the FDA signaled a significant paradigm shift, highlighting the increasing cybersecurity risk as medical devices become interconnected and offering recommendations to consider (including what information to include in FDA medical device premarket submissions for effective cybersecurity management). In January 2016, the FDA released post-market guidance[2] outlining its cybersecurity expectations for medical device manufacturers regarding "post-market surveillance" of their products. The guidance includes a recommendation that cybersecurity be addressed throughout the product life cycle.

Similarly, industry groups such as the Association for the Advancement of Medical Instrumentation (AAMI) have also released security risk management guidance for connected medical devices.[3] This guidance is affecting how medical device manufacturers are thinking and addressing cybersecurity issues, both for devices still in the pipeline and legacy devices that are already in the field.

Security by design

All this guidance is prompting device manufacturers to bolster their security practices. Manufacturers are taking steps to secure devices prior to deploying them, and they're conducting technical security testing and security risk assessments on devices while in development. By working with product engineers and technology leaders, companies can apply industry-leading risk management practices to connected medical devices throughout the product development life cycle (PDLC). These include practices to bolster product quality and safety (e.g., ISO 14971), as well as to identify, protect, detect, respond to, and recover from medical device security threats (e.g., AAMI TIR57).

Incorporating cybersecurity practices into the PDLC is often referred to as "security by design." This approach helps manufacturers design a device from the ground up to be secure, versus adding security features after the device has been delivered to market. The methodology considers many factors—including new regulations and guidelines, the current threat environment, and technical testing results—as the device is being designed, built, and tested. But security by design isn't enough. Staying ahead of adversaries in the evolving, connected medical device landscape requires continuous identification, assessment, and remediation of risks.

Incorporating cybersecurity practices into the PDLC is often referred to as "security by design."

Incorporating a three-layer defense

As discussed in Deloitte's recent ***Wall Street Journal*** article, "Managing Medical Device Security Risk," one leading practice is to establish a three-layer system to defend against cybersecurity threats.[4] This three-layer defense is made up of:

1. Documentation hierarchy
2. Product security risk management
3. Security event and incident handling

The first step is to establish a medical device documentation hierarchy, turning institutional knowledge into formal policy for directing medical device security activities. IT and medical device security leaders can apply standard quality management approaches to cybersecurity. They can also provide a platform of standards, procedures, and detailed work instructions/templates to guide IT and medical device security professionals and engineers.

The second step is for IT and medical device security leaders to partner on risk management activities for product security. The health care industry has decades of experience ensuring that medical devices are safe before they go to market (i.e., ISO 14971)—and they can take a similar approach to make sure devices are cyber resilient (i.e., AAMI TIR57). Activities to manage security risk throughout the device life cycle can help identify, measure, and mitigate threats—and they can inform the board and other key stakeholders about the risk landscape.

The third step is for IT and medical device security leaders to conduct thorough security event and incident handling activities, including forensic investigations to uncover breach sources, reduce exposure and reputational impact, and inform risk assessment and policy. Gathering intelligence about who attacked, what they did, and how they did it can help companies limit their damage, manage their response, and adapt for the future. These three layers of defense can collectively address the risks presented by connected medical devices while protecting patient and corporate assets.

Taking action now

Companies should consider taking the following actions as they move forward:

- Conduct security awareness training on the FDA's pre- and post-market guidance (and supporting artifacts)
- Ensure the cybersecurity team has a seat at the table with decision makers from product development, procurement, and sales throughout the product life cycle
- Establish a product-focused corporate cybersecurity organization to help implement cybersecurity processes universally across the enterprise
- Adopt and integrate TIR57 risk management principles for medical device security into the organization's product security program
- Embed security requirements from the FDA's premarket guidance into the quality management system (QMS) or equivalent document hierarchy, with appropriate governance and oversight
- Assign people to implement and execute security processes and train them appropriately
- Leverage outside expertise for medical device security risk assessments and technical security testing

These three layers of defense can collectively address the risks presented by connected medical devices while protecting patient and corporate assets.

Pending changes to the EU regulatory requirements

Last year we reported on the pending changes to the European Medical Device regulations. The trinity of current and long-standing directives—Medical Device Directive (MDD), In Vitro Diagnostic Medical Devices Directive (IVDD), and The Active Implantable Medical Device Directive (AIMD)—were being replaced by a pair of regulations: the EU Medical Device Regulation (MDR) and the EU In Vitro Diagnostic Regulations (IVDR). In May of 2017, both the MDR and the IVDR entered into force. After almost a decade of development and negotiation, the new regulations will help address advances in medical device technology and include:

- Reclassification of some technologies and the inclusion of others that were previously exempted from regulation, as well as classification of software
- Increase in the oversight of the medical device industry through enhanced authority of the Notified Bodies (NB) and independent review by the Competent Authorities of NB certification of certain high-risk devices
- Elevated clinical requirements for higher risk devices
- Imposition of more extensive post-market surveillance for many devices, including the use of Unique Device Identifiers (UDI) and posting of data into an enhanced European Databank on Medical Devices (EUDAMED) with greater access for interested parties, such as patient groups
- Higher focus on control of a manufacturer's supply chain and the inclusion of other entities, such as importers and distributors, under the regulation

As regulations, not directives, the MDR/IVDR will go into effect for all EU member states and don't need to be adopted by individual members, which can help ensure uniformity. The MDR has a three-year transition period, and the IVDR has a five-year transition period. During the transition, manufacturers will need to implement significant changes to their quality management systems. It will also be critical to work with vendors, such as distributors, to ensure that they also implement changes to their quality systems and organizational structures to comply with the new law.

Finally, since regulatory change doesn't occur in a vacuum, the new EU MDR must also be addressed in light of other concurrent regulatory developments, such as ISO 13485:2016 and the Medical Device Single Audit Program (MDSAP). The transition period for ISO 13485:2016 is already underway and ends March 2019. MDSAP, which has been adopted by Australia, Brazil, Canada, Japan, and the United States, is currently being monitored by the EU, WHO, and others. While participation in MDSAP is still optional in most local markets that have adopted it, MDSAP certification will become mandatory in Canada in 2019. The Health Canada website[5] states: These changes aren't pending. They're in play and will become mandatory in a very short period of time. While compliance with all these changes can provide a strong economic advantage for the savvy organization, careful planning and efficient execution are essential. And the clock is ticking.

> Health Canada intends to implement MDSAP as the sole mechanism for manufacturers to demonstrate compliance with the quality management system requirements of the Medical Devices Regulations (the Regulations). MDSAP will replace the current Canadian Medical Devices Conformity Assessment System (CMDCAS) program, even in situations when a manufacturer intends to sell only in Canada…As of January 1, 2019, only MDSAP certificates will be accepted.

21st Century Cures Act

The 21st Century Cures Act[6] (the Act) is intended to address a significant number of current challenges within the life sciences industry, including:

- Reduction of barriers to research collaboration
- Incorporation of the patient perspective into the drug development and regulatory review process
- Earlier identification of diseases through personalized medicine
- Modernization of clinical trials
- Elimination of regulatory uncertainty for the development of new medical applications

It also includes provisions to incentivize the development of drugs for rare diseases, invest in science and the next generation of investigators, and support the bio-medical ecosystem to accelerate discovery of new cures.

The Act contains changes in regulatory oversight that will likely affect many aspects of the industry's product life cycle, including:

- Clinical trial design and data collection
- Patient-focused drug development
- Drug manufacturing
- Premarket reviews of break-through devices
- The medical device regulatory review process
- The regulatory definition of medical device software
- Health information technology

The accelerated use of such technologies as biomarkers, human genome mapping, mobile medical applications, cloud computing, and social media are having a profound effect not only on consumers but also on biopharmaceutical and medical device organizations and federal regulators. To keep up with the fast pace of emerging technologies in the life sciences marketplace, the Act was signed into law on December 13, 2016.

Provisions of the Act relevant to the life sciences industry are within Titles I–IV (Innovation, Discovery, Development, and Delivery), which have numerous provisions primarily affecting the National Institutes of Health (NIH) and the FDA. For example, Title I of the Act (Innovation) establishes NIH funding of $4.8 billion over 10 years for the Precision Medicine Initiative (PMI), the Brain Research Through Advancing Innovative Neurotechnologies Initiative, cancer research, and regenerative medicine using adult stem cells. It also establishes FDA funding at $500 million over 10 years to give patients faster access to drugs and medical devices while maintaining current safety and effectiveness standards. The FDA delivered a draft work plan to Congress on June 9, 2017, outlining how the agency will allocate this funding.[7]

Title II (Discovery), Facilitating Collaborative Research (Subtitle F Sections 2061, 2062), promotes a National Neurological Conditions Surveillance System and calls for improved methods for prevention, diagnosis, and treatment of tick-borne diseases. Life sciences companies working on neurological research, as well as those involved in Lyme disease treatments, may benefit. Similarly, promoting pediatric research through NIH (Subtitle G, Sections 2071, 2072) establishes national and global pediatric research networks to pool resources related to rare pediatric diseases. Such a network may likely be helpful to organizations focused on the pediatric market.

Title II also encourages advancement of PMI, a research effort to prevent and treat diseases based on lifestyle, environment, and genetics. Subtitle B, Section 2011 calls for the application of genomic technologies to better understand diseases. Industries developing such technologies may be able to leverage this initiative.

Title IV (Delivery), ***Interoperability*** (Section 4003), focuses on the interoperability of health information technology (Section 4006) to empower patients to access electronic health information. These provisions involve a very large ecosystem of devices, information systems, and networks, including new technologies such as cloud computing. This may create opportunities for data analytics, data networking, and data security.

Many of the provisions that affect life sciences companies are delineated in Title III (Development). Specific provisions include:

- Patient-focused drug development
- Advancing new drug therapies
- Modern trial design and evidence development
- Patient access to therapies and information
- Medical device innovations
- Improving scientific expertise and outreach at FDA

The accelerated use of such technologies as biomarkers, human genome mapping, mobile medical applications, cloud computing, and social media are having a profound effect not only on consumers but also on biopharmaceutical and medical device organizations and federal regulators.

An in-depth look at the Cure Act and its various provisions can be found at: https://www2.deloitte.com/us/en/pages/life-sciences-and-health-care/articles/twenty-first-century-cures-act-life-sciences-development.html

Customer relationships: Taking stock and managing risk

After years of focusing on the life sciences industry's relationships with physicians, including dozens of corporate integrity agreements (CIAs) centered on alleged off-label promotion or potential kickback arrangements, government regulators, public advocates, and the media are increasingly focusing on initiatives and relationships between pharmaceutical companies, their distribution channels, and health care providers.

A key question for companies to ask is: What controls are in place to help mitigate the regulatory risk with current relationships and to identify the next risks that could emerge in the never-ending search for creative approaches for improving product development and patient care?

Here are five controls for companies to consider:

1. **Justify the need.** *Assess current relationships and establish or update standard processes to help ensure the arrangement with every customer can be appropriately justified.*

The industry has come to understand the idea of a "needs assessment," a concept that was first included in the CIAs with several of the world's leading orthopedic medical device manufacturers. Subsequent settlements with pharmaceutical manufacturers have included similar requirements, whereby, at an aggregate level annually (e.g., annual needs assessment) and per each activity (e.g., rationale documents), a company assesses the bona fide need for each customer arrangement, as well as the number and type of HCPs involved (e.g., specialist and qualification tier)—and the frequency of the activity—to validate a legitimate business need prior to commencing the engagement.

Moving forward, it's important to justify each customer engagement and manage that justification throughout the life of the contractual terms. Companies may want to reevaluate how they're determining the need for:

- Negotiating and drafting their third-party distribution agreements to properly reflect the specific activities the third parties will be performing
- Metrics for measurement (e.g., compliance checklist)
- Expected deliverables (e.g., proof of performance) that will support fair market value (FMV) payment for these services

2. **Catalog all customer activities.** *Include in the annual risk assessment a catalog of business arrangement types the company has in place with all customer types with which it does business, including specialty pharmacies.*

In addition to assessing the legitimacy of every activity, the risks associated with those activities should also be routinely assessed. As a participant in the US federal health care system, a company faces potential scrutiny for any type of arrangement it makes with any entity involved in the prescribing or dispensing of its products. Most companies have numerous types of existing arrangements with prescribers and dispensers of its products, and individuals within the company who are involved in commercializing products will continually be challenged with creating new types of arrangements that support improved health care delivery. Companies need a catalog or database of all such customer activities to leverage in an ongoing manner as part of the current and future risk assessment process.

While there are multiple facets to a strong risk assessment process, effectively summarizing the triangle of company products, customers (e.g., physicians, specialty pharmacies, other distributors), and associated business arrangements is a critical first step. Each time a risk assessment process begins, the summary should be revisited and updated based on input from commercial, medical, clinical, financial, legal, and compliance colleagues. This doesn't guarantee risk prevention, but not maintaining such a list may greatly increase the chances of discovering such risks when it's too late to mitigate them quickly.

3. **Justify the value.** *Establish or update standard processes to help ensure that FMV is being paid for any bona fide service provided to the company as part of a contract or engagement.*

In addition to justifying the conduct of every activity with a customer, it's also required by the Office of the Inspector General to justify the value of every arrangement and to validate that the company has documented policies and procedures to determine the FMV. Other considerations regarding

the bona fide nature of the services may also affect government price reporting calculations. Consider a review of the payment process to ensure that contracted services were actually performed.

4. **Consider other in-process controls.** *Consider implementing other specific controls to manage off-label and anti-kickback risks (e.g., reviewing compensation plans, utilizing inclusion/exclusion lists).*

Just as sales representatives shouldn't be given incentives to sell to physicians whose specialties don't align with the indications on product labels, scrutiny should be given to the idea of any employee or agent of a company being incentivized for the volume of patients receiving reimbursement assistance and clearance for their company's drugs. That volume should be driven solely by physician prescriptions to their patients.

The CIAs of the last decade provide guidance to some specific controls that can potentially be applied. For example, employees assisting with prior authorization and other patient support services, either directly or through a third party such as a specialty pharmacy, should have their compensation plans closely reviewed and approved by the company's legal department on an annual basis. If leveraging a third party, contract terms should consider the company's right to review incentive compensation plans as one of its controls in the overall effort to mitigate risk with such relationships.

5. **Audit and monitor.** *Consistently include the full range of products, customers, and activities in the company's auditing and monitoring efforts.*

The first four controls help mitigate risk because they're built into the processes at the earliest stages of various business activities. Compliance auditing and monitoring is another control that allows for assessing risk as activities are taking place or after they have taken place. If a company has specialty pharmacy relationships, for example, and is uncertain about the risks associated with them, auditing one or more of those contracts should provide an indication of the risks at the level of the specialty pharmacies and/or within the company's systemic processes for establishing and managing those relationships.

The auditing and monitoring plan should be derived annually from the risk assessment output, such that identifying new untested activities that carry risks can then be included in the subsequent year's auditing and monitoring plan for more in-depth review. In turn, the output from a quality auditing and monitoring program should be used as input to the next cycle of risk assessment, such that a virtuous cycle of continuous improvement is created and maintained.

Managing customer relationship risks

Implementing continuous and consistent risk assessment processes designed to ask questions across the entire customer continuum (i.e., all activities conducted with all customers for all brands, all types of clinical research agreements, collaboration agreements, etc.) should help mitigate inherent regulatory risks when working with customers. Conducting appropriate monitoring controls throughout the life cycle of each customer relationship (from strategic planning and budgeting to payment and reporting) should help as well.

In turn, the output from a quality auditing and monitoring program should be used as input to the next cycle of risk assessment, such that a virtuous cycle of continuous improvement is created and maintained.

FDA ORA program alignment

The FDA Office of Regulatory Affair's (ORA) program alignment was an initiative announced by then FDA Commissioner Dr. Margaret Hamburg on September 6, 2013, in response to the increasing technical, global, and legal challenges facing FDA scientists, investigators, and compliance officers. Scientific innovation in biotechnology and software requires greater understanding by regulators. Medical mobile applications, cloud computing, and combination devices represent just a few examples of the increasing breadth and complexity of regulated products. Regulatory authority and mandates have expanded recently with legislation such as the Family Smoking Prevention and Tobacco Control Act (2009); Food Safety Modernization Act (2011); and the Food and Drug Administration Safety and Innovation Act (2012), which includes the Generic Drug User Fees Amendments of 2012, Drug Supply Chain Security Act (2013), and the 21st Century Cures Act (2016). All these acts contain provisions requiring the FDA to publish guidance and promulgate new regulations years after acts have been signed.

Since 2013, the FDA has been working on a set of core operational changes to effectuate program alignment:

- Specialization, to the extent that it hasn't been achieved, across FDA's inspection and compliance functions, which enables the FDA to mirror, adapt to, and track the continuing program-based specialization within the FDA's regulated industries and the demands of new legislation
- Training that's developed collaboratively by ORA and the Centers and leads to the development of competency requirements, training curricula, certification/qualification/accreditation processes, performance assessments, and a continuing education program that enables FDA to enhance and maintain its experienced workforce
- New work planning that:
  - Improves the FDA's selection of firms, inspection frequency, and compliance efforts
  - Is based on risk factors, public health outcomes, past inspectional history, and operational experience
  - Is reported through performance-based metrics clearly demonstrating public health and compliance outcomes
- Compliance policy and enforcement strategies that are clear, current, outcome-based, and effectively communicated in order to enhance the FDA's ability to protect public health and to exercise effective and efficient industry oversight
- Laboratory optimization that increases specialization; fosters program alignment and collaboration between the Directorates, ORA, and the Centers; and enhances efficiency within the current laboratory configuration
- Center and ORA practices, processes, and resources that are effectively aligned in order to support ORA's implementation of FDA's commodity-based and prevention-focused regulatory programs

Each FDA commodity-specific Center collaborates with ORA on yearly action plans incorporating the above core changes. For example, the initial Center for Device and Radiological Health (CDRH)/ORA medical device action plan focuses on enhanced device quality. Enhanced device quality involves a paradigm shift from reaction to problems after they occur to a model that focuses on the quality attributes of devices in order to prevent safety and efficacy issues before they occur. Now, quality in this context relates not only to regulatory compliance but also to the totality of features and characteristics that bear on the ability of a device to satisfy fitness for use, including safety and performance. Supporting innovation means facilitating development, approval of, and access to even safer and more effective devices, as well as support promising new technologies. Examples include providing clear and consistent guidance, sharing policy on emerging technology, and providing education and support to organizations through various engagement opportunities. Finally, increased consideration of patient benefit means any FDA decisions and policies should consider both inspectional and compliance history, as well as an overall assessment of the benefit versus risk to patients and consumers.

ORA specialization was implemented on May 15, 2017, where a program based-management structure (Drug, Device, Biologic, Bioresearch Monitoring, Food, Tobacco, Imports, Laboratories) was stood up, replacing the traditional geographic managed regions (Northeast, Central, Southeast, Southwest, Pacific).

Next-generation transparency reporting and expert engagement

Throughout the growth of the modern life sciences industry, collaboration between industry and the medical and payer communities has helped to advance scientific exchange and improve patient outcomes. To enable the industry to engage experts for their experience and insights, various contract mechanisms have been developed. These mechanisms tend to vary by function and market.

With the advent of transparency reporting and the continued expansion of requirements—both geographically and in terms of content—the industry faces the challenge of capturing spend data and providing a consolidated, holistic view. To meet reporting requirements and deadlines, many companies have cobbled together data and often resorted to manual labor when technology couldn't deliver what was needed. This brute force approach, however, isn't sustainable. Also, while many companies have implemented first-generation solutions and operating models to try to ease the reporting burden, these solutions have at times struggled just to meet the requirements, let alone generate valuable business and compliance insights and benchmarking from the data.

Most companies acknowledge the value of using transparency and engagement data for compliance monitoring, peer benchmarking, and general business analysis. But scarce resources, deficient technology, and disparate operating models and regional requirements make it challenging to harness this information. Furthermore, the systems and operating models in place today are costly to maintain, and even more costly to upgrade to meet new reporting obligations and achieve the desired advanced analytical capabilities.

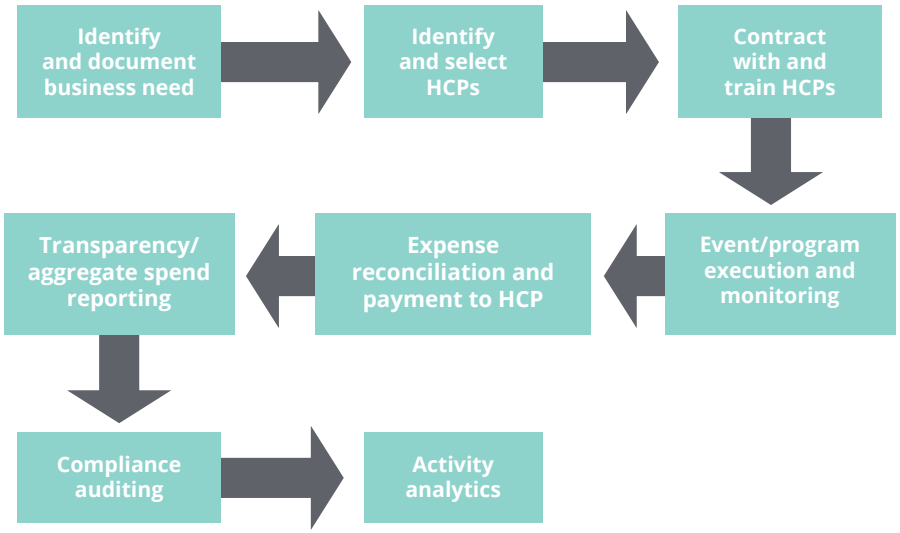
Leading manufacturers are pushing into the next generation of transparency reporting and expert engagement, building on overall industry trends to deliver improved efficiency, business value, and compliance through a holistic approach.

Most companies acknowledge the value of using transparency and engagement data for compliance monitoring, peer benchmarking, and general business analysis.

Technology

Managing expert engagement is a complex workflow that includes many steps, from initial identification of the need for engagement, through event/activity completion, to compliance auditing and analytics. This complexity increases when global solutions are considered because local regulations introduce complexity to the workflow and cross-border approvals require alignment on definitions and review process steps. (Figure 1).

Figure 1: Sample HCP engagement management workflow



Transparency reporting is both a reflection and output of a company's interactions in the marketplace. And the accuracy of transparency reporting is only as good as the engagement management process that precedes it.

Although full automation of the end-to-end HCP engagement process isn't common today, this likely will change as companies seek a more proactive approach to managing the totality of their external relationships and as they increase their monitoring and controlling of compliance risk.

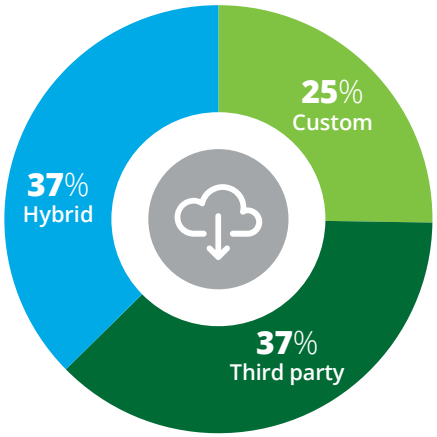
Companies with the most advanced and standardized engagement processes tend to use workflow management technology and processes to enable the component parts of expert engagement, and there's a trend toward centralizing systems.

Our experience has shown that improved compliance controls and more efficient operations can be achieved through automation. To make it happen, the priority and sequencing of automating processes should be agreed upon, technology options to drive automation should be carefully analyzed, and a road map for implementation should be developed.

Today, three technology approaches for transparency reporting are roughly equal in popularity: custom, hybrid, and third party. (Figure 2).

Our work with clients indicates that custom solutions were often initially pursued several years ago because third-party solutions didn't adequately meet user needs. Custom solutions tend to receive the highest satisfaction ratings, followed closely by hybrid solutions. However, the cost to upgrade and maintain a custom solution is generally higher than for a third-party solution. The cost savings associated with third-party systems—combined with technology advancements—will likely lead more companies to adopt third-party and hybrid systems in the future. A hybrid solution offers aggregation of a large variety of source data for improved processing efficiency, along with the ability to rely on a third party to monitor changing regulations and maintain updated report formats.

Figure 2: Technology for transparency reporting[8]



Operating model

Centers of excellence (CoEs) are being formed to gain better visibility into company risk related to engaging HCPs. They can also help in the creation of consistent processes and in more efficient use of resources.

Governance of transparency programs continues to shift within organizations. These shifts are being driven by the addition of transparency reporting requirements outside the United States and by companies establishing CoEs. Although most companies still assign responsibility for governance to the compliance function, some have moved this responsibility to the finance or medical function. Finance has strong controller capabilities, and the medical function often has a significant role in country operations beyond the United States. In addition, the medical function generally owns HCP FMV tiering (and the relationships with the external experts).

CoE headcount can vary significantly based on the scope of activities included. Tasks that tend to be most appropriate for CoEs are those that are consistent across countries and that can be made routine. Examples of roles often performed by CoEs include data comparison and remediation, report creation and filing, policies and procedures development, and training.

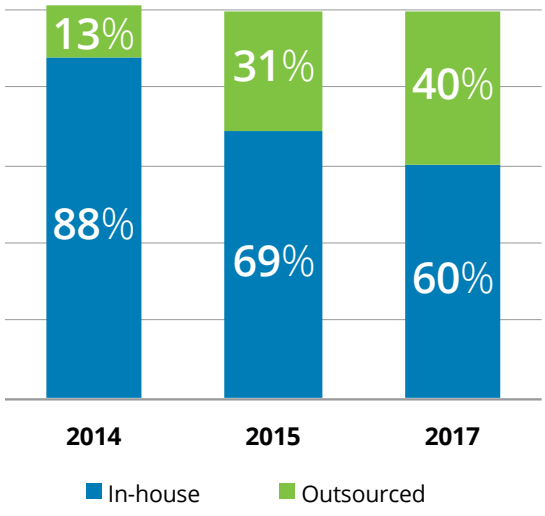
Outsourcing transparency reporting operations is an increasingly common way to improve data quality and reduce overall costs. (Figure 3). Also, outsourcing provides an opportunity to deploy scarce internal resources to elements of a company's transparency program that are business-critical and higher-value, while allowing specialized teams outside the organization to handle routine operational tasks. If current trends continue, an increasing number of companies may likely outsource a portion of their reporting operations within the next one to two years. As part of this shift, companies might consider paying third-party providers on a volume basis with service level agreements (SLAs) in place to control timeliness and cost.

Where to go from here?

Whether facing the challenge of improving transparency reporting as a stand-alone issue or as part of a broader focus on expert engagement, leading companies are continuing to evolve their thinking and solutions in this area. However, one thing that's already clear is that there's no "one size fits all" approach to meeting the requirements or to generating the valuable business and compliance insights made possible by improved transparency and expert engagement data.

For individual companies—and the industry as a whole—the focus of transparency reporting is shifting from simple compliance to opportunities for improved efficiency, effectiveness, and value creation. Although achieving compliance across numerous jurisdictions remains a challenge, the move toward sustainable operating models and increased business insight provides companies with many questions and opportunities to make transparency and expert engagement management more than just a cost of doing business.

Figure 3: Outsourcing of transparency reporting is on the rise



Modernizing compliance

Compliance is an enabling component for any regulated industry. In life sciences, it's a cornerstone of both product development and commercialization, giving the business a framework by which commercial objectives and patient access can be appropriately maximized. Consequently, many manufacturers are no longer satisfied with merely adhering to the "rules" set forth by compliance. Instead, they're adopting the values and principles of these standards as a way to guide the business.

Effective compliance management is increasingly becoming a source of competitive advantage. Moving forward, compliance officers will need to demonstrate the value their function contributes to the organization. They will also need to demonstrate the effectiveness of the organization's compliance approach to external stakeholders. The current compliance landscape of regulatory pressures and internal challenges often leads to poor decision making, integration, and execution. Modernizing compliance through the use of technology, with a focus on efficiency and value creation, can shape the future compliance landscape and transform how the compliance function is viewed.

Traditional compliance functions often took a rules-based approach to guiding business colleagues. They also used monitoring to identify and remediate deviations from standards. Through modernization, the compliance function is moving toward being predictive and risk intelligent, acting as an enabling partner to the business, striving for operational excellence, and providing greater value to the company.

Compliance function maturity model

The foundational aim of any compliance program will always be simple: prevent, detect, respond to, and remediate risk. Today, a foundational compliance program already does far more than that theoretical minimum. However, it remains at one end of a progression, with each compliance function able to determine how far it should evolve. But to achieve the goal of creating value with compliance, few organizations can stick with the status quo. As an organization moves up the capability curve, much more becomes possible.

While almost every compliance program establishes and oversees core tasks—such as risk identification and assessment, testing, monitoring, and governance—a "modernized" compliance program delivers on a more complex level.

Top-notch compliance functions are:

Strategists	Communicators	Risk managers	Stewards
Provide compliance leadership for the business and the organization	Promote a culture of compliance and integrity throughout the organization and communicate this vision to all relevant stakeholders	Direct all aspects of the compliance risk management program, from assessment to implementation of mitigation plans	Assume ownership and identify accountability for reputation and compliance risks, fortify controls, and build relationships and trust with stakeholders

Benefits of modernizing compliance

A modernized compliance function can be an organization's most finely tuned way to monitor what's going on inside its four walls, as well as what's approaching from outside. Some may view this as the addition of a "sixth sense" that lets the organization perceive risks and opportunities in a new and more precise way. In the wake of this transformation, knowledge isn't just gathered; it's made useful through enterprise-wide access to dashboards that put risk data, analytics, and key performance indicators in the hands of decision makers at the moment they're needed.

Beyond sense is action, and a modernized compliance function can also serve as an extra set of hands. Given a seat at the strategy table, the modernized function can not only detect risks that may affect the organization in negative ways, but it can also steer the organization toward new areas of opportunity. Also, modernized compliance can help reduce both the cost and level of regulatory scrutiny. And it can make operations more efficient and increase consumer confidence in game-changing ways, not just incremental ones.

In part, this is because compliance is (or can be) one of the most data- and analytics-rich parts of the enterprise. Organizations invest a lot of money capturing and processing data to satisfy regulators, and this data can provide value to the organization.

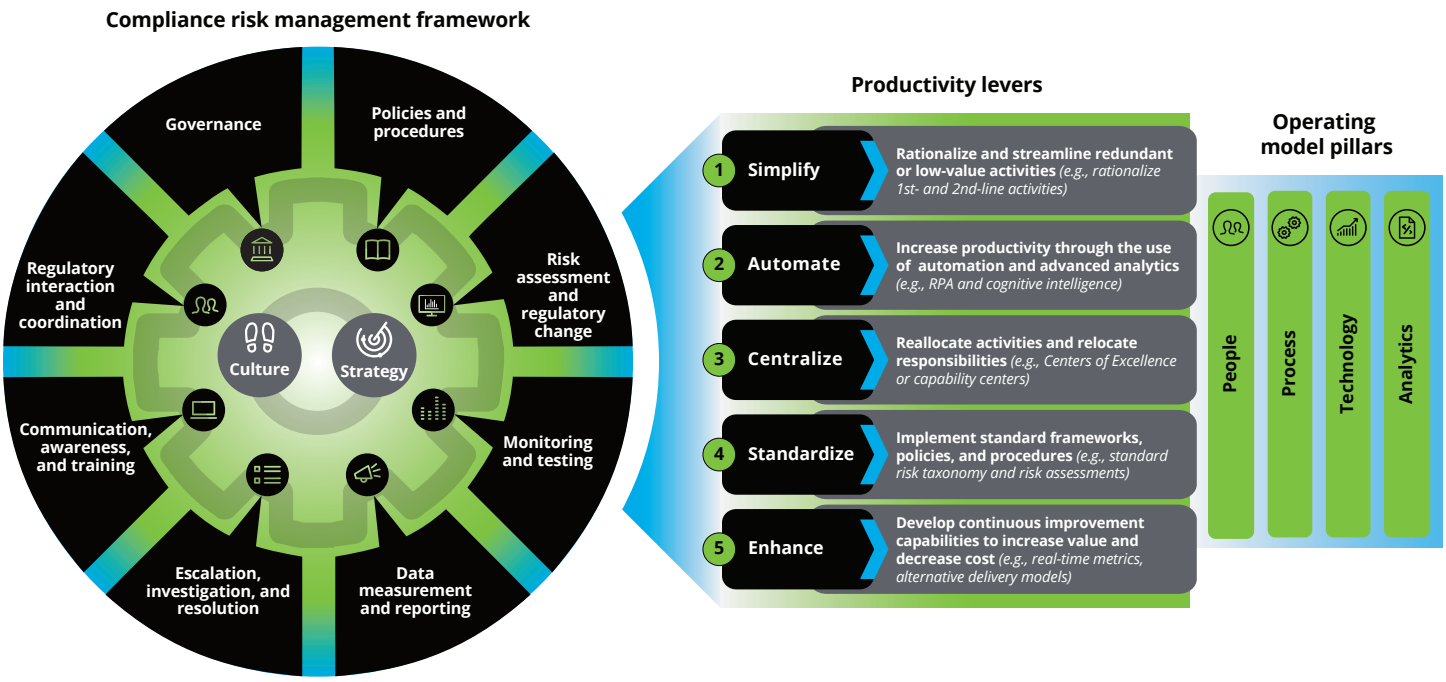
✓	It builds culture, ethics, and appropriate incentives into compliance, and vice versa, recognizing that while written rules can govern transactions, it takes a deeper-rooted understanding to instill a sense of appropriate behavior
✓	Instead of merely identifying roles, a modernized program seeks a more insights-focused, process-oriented talent base and cultivates people across the organization who fit the new normal
✓	To the three classical operating model and capability areas of "people, process, and technology," modernized compliance adds a fourth: analytics
✓	The reach of—and reliance on—its technology and analytics capabilities is wider and more comprehensive

The degree to which an organization modernizes its compliance program varies based on a number of factors, such as the organization's overall maturity, values, tone at the top, risk profile, and overall regulatory environment position.

Benefits of a modernized compliance program include:

	Transformative change: Reengineer core processes and automate the function to be more proactive and predictive; modern enterprises need top-of-the-house strategies and reliance models.
	Flexibility: Rapidly scale up or down, depending on the nature of the compliance and/or business issue.
	Increase to capacity: Reengineer traditional resource model and allocation methods and use deployment of technology, analytics, managed services, and offshore to ensure proper use of resources.
	New competencies: Compliance professionals are elevated to true business partners and advisers.
	Potential cost reduction: Cost reduction opportunities exist by creating efficiencies and seeking ways to be more effective with increased capacity across the organization through better use of technology and resource allocation.
	Enterprise-wide view of risk and compliance: From predicting and sensing to acting and monitoring, the lines between these formerly separate operational areas and compliance functions are disappearing quickly.

Driving compliance productivity through compliance modernization



Compliance modernization isn't a finite destination, it's a journey—an evergreen process that strives to embrace change and flexibility. It also strives to deploy all pillars of an efficient and effective operating model to meet the challenges of the market, guide the business to a distinct competitive advantage, and position it as an ethical market leader.

Transformation

Moving along the compliance evolution continuum and unlocking the potential to create material and strategic value is a process. The end-to-end compliance risk management framework and related operating model have evolved to meet rising expectations, providing a standard way to help design, assess, implement, and continuously improve and modernize an organization's compliance function.

One way to chart, execute, and measure the modernization process is to review the key steps:

- **Determine** the desired modernized state for the compliance risk management program
- **Perform** an assessment of the existing compliance program against the desired state
- **Prioritize** areas that need to be addressed based on the results of the assessment, level of risk, and expected change to the organization
- **Develop and update** the overall vision/mission for compliance in order to align it with the desired modernized state
- **Develop and update** the compliance strategy, confirm it aligns with the company's overall strategy, and determine appropriate measures of effectiveness
- **Determine** what levers (e.g., investments, initiatives, resources, tools, technology) are needed to achieve the desired modernized state

To stay at the cusp of the industry—and to lead their respective therapeutic focus areas and appropriately maximize their development and commercial objectives—life sciences companies must be clear and deliberate in modernizing their compliance function and creating the next generation of compliance capabilities. The time to act is now.

Identification of medicinal products (IDMP)

IDMP is a set of five ISO standards, supported by European legislation and regulation, which allows for unique identification of regulated pharmaceutical products throughout their entire life cycle, from development to authorization to marketing. The standards facilitate exchange of medicinal product information in a robust and reliable manner.

The European Medicines Agency (EMA) is rolling out legislation covering core components of IDMP master data: Substances, Products, Organizations, and Referential (SPOR). IDMP SPOR is intended to align with other EU regulatory directives and to ultimately extend globally—with other regulators and regions leveraging the standards. The initial rollout of Organizations and Referential took place in 2017, with the implementation expected to become more robust in the coming years. However, the guidance and timelines for Product and Substances, which are the bulk of IDMP, continue to be delayed for a few more years.

Most companies have invested in IDMP through readiness assessments to understand IDMP's role in their data ecosystems and the anticipated impacts to processes throughout the product life cycle. Larger companies envision IDMP as a multiyear business process transformation initiative.

Companies are responding to the announced delays in different ways. Some are waiting until clear guidance, timelines, and implementation specifications become available before continuing further. Others are leveraging the delays and taking a more strategic approach to centralizing and standardizing regulated product information. This strategic approach includes:

1. **Moving forward with product master data management (MDM) efforts.** Since the data required for IDMP is distributed across multiple departments and systems within R&D, manufacturing, and regulatory affairs, many companies have begun and are continuing to implement MDM solutions. Implementing MDM is a complex and time-consuming journey that includes process, governance, and system changes. "Master Data Management: Building Readiness for Regulations," written by Deloitte Consulting LLP, offers more information on the benefits of implementing product MDM, as well as the steps required.[9]

2. **Moving data from documents into the organization's regulatory information management (RIM) system.** Many, but certainly not all, IDMP Iteration 1 attributes are regulatory in nature and can be added to the RIM system. This makes the data more accessible and can ease the burden of preparing for IDMP when IDMP is required in the future. This requires that companies develop processes and governance to manage and maintain changing product data.

Moving forward with an MDM program and migrating data from documents to a RIM system both require time-consuming activities that include:

1. **Identifying the authoritative source of truth for each data element.** Today, much of the data resides in multiple systems. To avoid maintaining duplicate data, evaluate the need for a single source of truth and then establish new systems or consolidate/integrate existing ones.

2. **Extracting data from structured documents.** It's estimated that much of the needed data is found in unstructured documents and forms. To tackle the challenge, companies should understand the best approaches, technologies, and timing for collecting information, checking quality, and curating the information in the future. They should also evaluate the need to establish new fields in new or existing systems to avoid collecting data from documents.

3. **Verifying the extraction occurs properly.** Develop processes and quality checks that verify the extraction process has properly occurred and that allow for corrections as necessary. Data submitted to regulators should be supported by processes that can be validated.

4. **Linking data from disparate sources.** Regulatory and manufacturing product data are often captured at different levels of granularity, making them difficult to link. Establishing common identifiers that allow information to be linked and queried across systems is critical.

5. **Developing and testing processes for maintaining the data in the new system.** Data collection isn't just a one-time activity. As the product life cycle "lives," so does the need to have processes in place to maintain updates to the data. Leading companies are designing processes and systems to enable efficient reuse of data from authoritative sources, leveraging automation and reducing manual data reentry.

6. **Enhancing data governance.** Implement or enhance data governance procedures to manage the definitions and standards associated with the data. Since the IDMP data covers many systems and processes, a paradigm shift from system owner to data owner needs to be planned for—along with the associated governance.

In particular, some companies are beginning to use advanced technologies, such as natural language processing (NLP) and cognitive computing, to accelerate the identification, extraction, and verification of data stored in documents.

The availability of ISO IDMP provides a blueprint that allows system and process owners to become "IDMP aware" and plan for future adoption. Having an agreed-upon strategy is critical as some vendors are building the IDMP data model into their systems, a move that's challenging the status quo of data ownership and information flow across functions and systems, typically impacting manufacturing/product life-cycle management/enterprise resource planning (ERP) solutions, as well as a host of RIM solutions.

Companies should take time to address the findings from their data and IDMP readiness assessments, while also looking for opportunities to harness innovation. In particular, some companies are beginning to use advanced technologies, such as natural language processing (NLP) and cognitive computing, to accelerate the identification, extraction, and verification of data stored in documents.

Case for quality

The FDA launched the Case for Quality in 2011 following an in-depth review of device quality data and feedback from both the FDA and industry stakeholders. The FDA's analysis flagged manufacturing quality risks and showed that organizations that manage those risks by driving quality across their enterprise have the following characteristics:

- More productive, both in manufacturing throughput and quality management
- Fewer complaints and investigations per batch
- Smaller quality organizations able to manage quality and safety effectively
- Lower quality-related costs than their competitors

Companies with an established quality culture are able to use the increased capacity that results from avoiding quality failures to accelerate device design, innovation, and introduction of new products to the marketplace.

The Case for Quality represents a major initiative to engage the medical technology industry and FDA in a collaboration to focus manufacturers and regulators on the design and manufacturing elements that have the greatest impact on improving product quality and patient safety. The FDA, in conjunction with industry representatives, is coordinating the work of four Case for Quality working groups: maturity model, metrics, product quality outcomes analytics, and competency.

The industry and the FDA realized that compliance and quality are two different things and that even increased inspections weren't necessarily improving quality. While strong compliance is essential for good and sustainable quality, compliance alone doesn't create good quality.

Discussions with quality leaders from the industry highlight several barriers to adopting innovative quality programs, including:

- **Low transparency**, driven by a lack of information for consumers and decision makers about comparative quality
- **Increasing complexity** of medical devices and usage environments, which is straining the current quality system infrastructure
- **Perceived misalignment**, between the regulatory framework and assurance of quality outcomes

The Center for Devices and Radiological Health (CDRH) has partnered with the Medical Device Innovation Consortium (MDIC) and the medical technology industry to pursue the Case for Quality. Meanwhile, the FDA, in conjunction with industry representatives through MDIC, is coordinating the development of a maturity model to encourage a shift toward patient-centricity and data sharing.

A maturity model assessment can help a company understand its true costs and effectiveness related to quality, and how much time it takes to do all the work around the 30-day notices. Such assessments often reveal that companies are not making innovative changes because they are too bogged down in routine activities.

Pricing and market access

Few areas in the US life sciences industry are getting more attention from the public, Congress, and regulators than pricing and market/patient access. The United States, unlike most other countries, has a multi-payer system that largely allows commercial prices to be set by the "free market." However, this market environment has been met by growing criticism that drug prices are creating an undue burden for patients and government programs alike.

The focus on this issue includes not only pricing and price increases, but also indirect activities associated with creating market or patient access. Various congressional committees, including the Senate Aging Committee and Senate HELP Committee, have focused on pricing. The Government Accountability Office (GAO) has been called upon to research the matter. US Attorneys offices and other investigative and enforcement parties are pursuing inquiries. And subpoenas and judicial action against manufacturers have been levied.

Given the challenges of generating revenues to fuel future, life-saving therapies while responding to growing scrutiny and evolving regulatory requirements, manufacturers must take steps to understand and manage this growing risk area that threatens their reputations (and potentially their finances).

Pricing and price transparency

Recently, there has been significant attention on drugs that are priced significantly higher in the United States than elsewhere. In a few instances, large price increases have been noted for drug products that were recently acquired by a different company. Also, scrutiny has been given to the price points at which government programs acquire or receive reimbursement for certain drugs.

As demonstrated by their regulatory actions, state governments believe the public has a right to know what factors are driving costs and price increases. Accessibility concerns have emerged after high entry prices or significant price increases drove patients who pay out of pocket (or have high co-pays) to seek other solutions, including substitutions for the original product.

The latest attempt to reduce drug prices is through improved transparency; specifically, requiring the disclosure of pricing actions and, in some cases, an explanation of price increases. Explanations may be required for price increases of any amount or for increases that exceed a certain percent over a defined time period. There are also reporting thresholds where pricing information would be required for drugs costing more than a certain dollar amount per year. Other price transparency requirements focus on selected product types, disease states, or prices given to specific payers. These criteria are state-specific.

The price transparency trend isn't limited to the US market; new requirements for transparency reporting are emerging in various countries around the globe. As in the United States, the scope of these requirements includes disclosing information about drug pricing as well as reporting payments and other transfers of value to health care providers and other organizations.

Market access and patient access

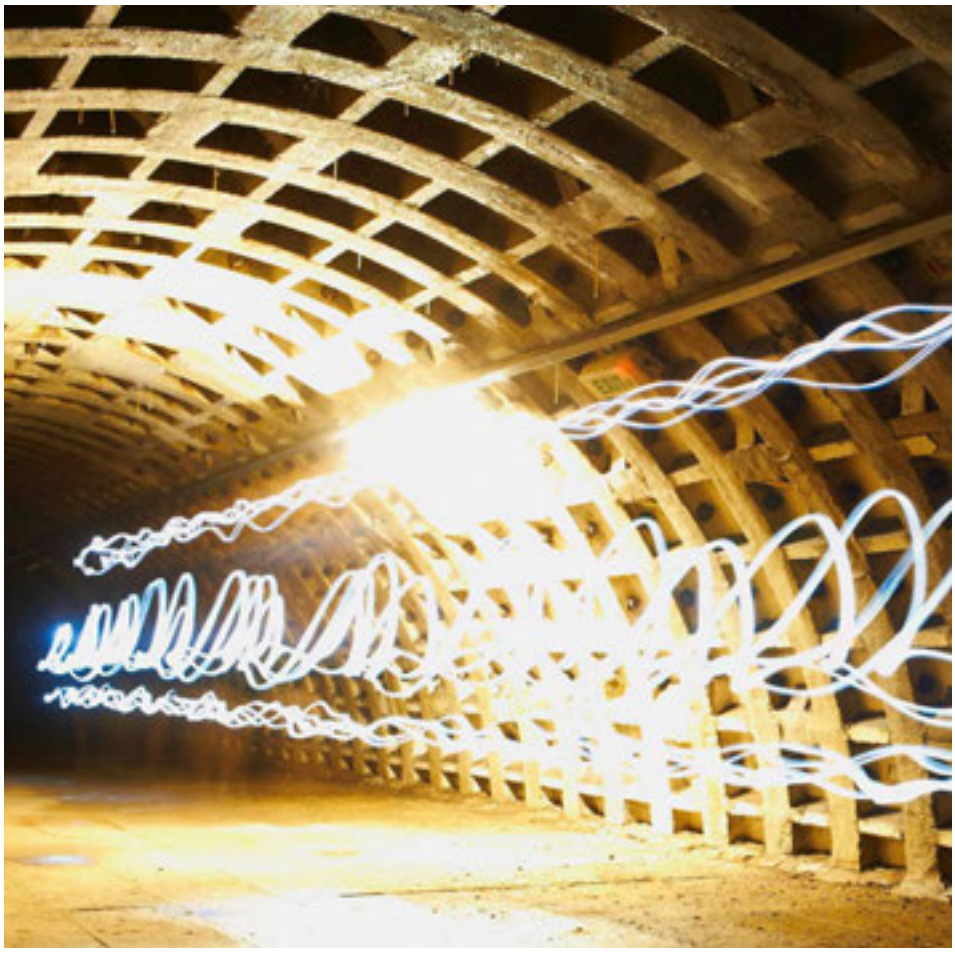
In the United States, as health care systems, reimbursement, and the products themselves have become increasingly complex, manufacturers have responded by creating market and patient access programs to help ensure that products are available to all patients who could benefit from them and that patients are provided with the support necessary to manage their disease states comprehensively and appropriately. However, regulators and enforcement bodies have recently called many of these access programs into question, claiming that manufacturers only provide the programs so they can charge higher list or wholesale acquisition cost (WAC) prices or inappropriately gain prescriptions. Also, claims have been made that some aspects of market and patient access put government programs at a disadvantage, create inappropriate incentives, or inappropriately drive patients to certain products.

Risks associated with patient and market access can be divided into two categories: those that affect realized price, and those that potentially create undue influence. Risks in the first category can pertain to prices realized by commercial payers, government payers, health care institutions, or patients. Also, they can arise in many forms, including contracted discount arrangements, co-pay programs, or coupons and vouchers. Although regulators and congressional bodies have specifically focused on how these programs might be linked to manufacturers setting higher list or WAC prices, the core of these concerns is that the government isn't receiving the best price or that all applicable discounts aren't being considered when establishing government price points.

With regard to the undue influence that may potentially be created by certain market and patient access programs, regulators and enforcement agencies have focused on the evolution of services in conjunction with product delivery. They have also focused on certain patient advocacy and access points—such as independent charity patient assistance programs (and the associated funding)—that might provide inappropriate incentives for patients or prescribers to use or prescribe certain products.

Looking ahead

In the future, concerns and trends related to drug pricing will likely continue, leading to more laws and more detailed and specific reporting requirements. In response, companies will need to dedicate resources to manage the operational aspects of complying with the reporting requirement, and, just as important, to manage public perceptions of the information that's disclosed.



340B drug pricing program

The 340B drug pricing program (340B) continues to receive heightened attention from life sciences manufacturers and the broader health care industry, with the size of the program continuing to increase at a significant rate—growth that shows no signs of abating in 2018.

The 340B program requires life sciences manufacturers to provide outpatient drugs to qualified and participating health care organizations at significantly reduced prices. As a condition for participation, a manufacturer must enter into an agreement with the Secretary of Health and Human Services to provide the discounted drugs to eligible entities. The 340B program has specific requirements for how manufacturers calculate and report prices:

- The 340B program provides one of the deepest discounts on biopharmaceuticals in the country.
- In 2016, 340B entities accounted for more than $16.2 billion in drug spend (5 percent of the US drug market).
- This represents a significant growth of about 35 percent in one year as compared to 2015's $12 billion drug spending figure.

The Health Resources and Services Administration (HRSA) Office of Pharmacy Affairs (OPA), which administers the 340B program, generated significant activity in 2017, including issuance and delays of new regulations and launch of a new online OPA Information System (OPAIS). Additional OPA activity and regulatory changes are expected in 2018, for which manufacturers need to prepare.

OPAIS online 340B ceiling price system

In September 2017, OPA replaced the previous online 340B database with the new OPAIS and launched the registration component, which has both public access sections and secured access sections for manufacturers and 340B covered entities. OPA has not yet announced the specific launch date of the pricing component of OPAIS, but manufacturers should prepare for the upcoming launch. Starting in July 2017, the OPA had communicated through national presentations to 340B stakeholders that the 340B pricing component of OPAIS was "coming soon." Manufacturers participating in the 340B program were previously required in December 2016 to sign the 340B program Pharmaceutical Pricing Agreement Addendum, in which manufacturers agreed to submit quarterly 340B ceiling prices to OPA via the online system. After the OPAIS pricing component launches, manufacturers will be expected to face onerous compliance requirements with a potentially short compliance implementation timeline. Such requirements include:

- Submitting pricing data—including Medicaid average manufacturer price, Medicaid unit rebate amount, and 340B ceiling price—through the secure OPAIS pricing application on a quarterly basis
- Performing OPA-assigned activities as requested, such as reconciliation of 340B ceiling prices when manufacturer-submitted prices don't match those calculated by OPA

340B ceiling prices validated by OPA will be published and made available to 340B covered entities on a quarterly basis via OPAIS, and manufacturers may only have weeks or days to complete the required quarterly activities.

In a July 11, 2017, OPA presentation at the 340B Coalition Conference, OPA described the OPAIS pricing component as receiving automated feeds of historical Medicaid average manufacturer and best price restatements from the Centers for Medicare & Medicaid Services (CMS), which in turn would generate restated historical 340B ceiling prices that would be published and made available to 340B-covered entities on OPAIS. This could have significant implications for manufacturers regarding refunds of overcharges to 340B-covered entities for any restated 340B ceiling prices that are lower than original 340B ceiling prices.

In a September 2017 webinar that Deloitte conducted for life sciences manufacturers to share OPAIS information, only 12 percent of participants indicated that their companies were well prepared for the changes. Fifty-one percent indicated that changes were in process, and 37 percent indicated that their companies had not yet begun or were still in the early stages of preparing for the changes.

To support compliance with the OPAIS registration component that's already in effect, manufacturers should ensure they have implemented the necessary activities, including:

- Monitoring to confirm that accurate manufacturer information is being maintained in the OPAIS registration component
- Developing procedures to address OPAIS registration component processes
- Training relevant personnel on OPAIS, leveraging OPA's online resources and the manufacturer's procedures

Also, manufacturers should make advance preparations for the forthcoming OPAIS pricing component launch, including:

- Defining processes related to OPAIS pricing submissions, questions from 340B-covered entities, and 340B ceiling price restatements and refunds
- Documenting procedures that will be in effect following "go live" of the OPAIS pricing component
- Preparing a 340B customer communication strategy and plan for internal stakeholders (e.g., account managers) and external stakeholders (e.g., wholesalers, distributors)
- Closely monitoring launch updates for the forthcoming OPAIS pricing component

340B ceiling price and civil monetary penalty regulations

Since issuing the 340B Drug Pricing Program Ceiling Price and Manufacturer Civil Monetary Penalties Regulation on January 5, 2017, HRSA has delayed the effective date of this final rule multiple times.

At the time of this writing, the effective date is July 1, 2018. As currently written, the regulations impose fines up to $5,000 on manufacturers for each instance where they knowingly and intentionally overcharged a 340B-covered entity. The regulations also address various requirements for manufacturers related to:

- Definition of "covered outpatient drug"
- Calculation of 340B ceiling price
- Calculation of provisional 340B ceiling price for new drugs
- Penny pricing

Updates to these regulations may be released by HRSA prior to the forthcoming effective date. The regulations as currently written are expansive and could have significant regulatory compliance, operational, and financial impacts for manufacturers. Manufacturers should start preparing for the aspects of the regulations that could take longer to implement, and they should have contingency plans in place prior to the July 1, 2018, effective date.

CMS Medicare Outpatient Prospective Payment System (OPPS) final rule

On November 13, 2017, CMS published its 2018 Medicare annual payment rule for outpatient hospital departments, ambulatory surgical centers, and home health settings. The rule was issued as a final rule with a comment period effective January 1, 2018. It included a 28.5 percent reduction of Medicare Part B reimbursement to disproportionate share hospitals (DSH) and rural referral center hospitals for separately payable drugs and biologicals purchased through the 340B program (from average sales price (ASP) plus 6 percent to ASP minus 22.5 percent). CMS's stated objectives include reducing out-of-pocket drug costs for Medicare patients and reallocating savings to all hospitals paid under the OPPS.

Legal action has been taken by 340B-covered entity providers. The 340B-covered entities and advocacy groups that oppose the final rule assert that the new reimbursement rate would deprive them of essential financial resources and threaten their ability to provide needed health care services to their communities.

The potential impact to manufacturers is to be seen following the final rule effective date and the 340B-covered entities' reactions to the reimbursement reduction. Reactions could include DSH and rural referral center hospitals choosing to purchase outside of the 340B Program following the effective date. Manufacturers should alert their internal stakeholders—including stakeholders who manage accounts with these types of 340B-covered entities—and monitor activity accordingly.

HRSA audits of manufacturers

At the 340B Coalition Conference in July 2017, OPA communicated that manufacturer compliance with 340B program requirements continues to be a focus area. HRSA plans to continue auditing manufacturers in 2018, and manufacturers should assess their audit readiness and prepare accordingly.

Focus on R&D: Expanded access programs and health care economic information

R&D organizations in life sciences are consistently challenged to increase productivity and pipeline throughput, but they must contend with the challenges of a changing regulatory landscape. The days when a company could rely solely on its quality assurance function to manage R&D-related regulatory compliance risks are over.

Industry go-to-market strategies and tactics have shifted to focus on the patient to an unprecedented degree, and government investigators have followed suit. As a result, the compliance function has become increasingly accountable for managing risks that touch R&D operations.

In particular, new legislation and new regulatory scrutiny have brought greater attention to two key areas: expanded access programs, and health care economic information.

Expanded access programs (EAPs)

According to Section 3032 of the Act, which became law on December 13, 2016, sponsors of clinical research must make their policies on evaluating and responding to expanded access requests publicly available. Although the law does not guarantee expanded access, it does require each company's policy to include:

- Company contact information related to the study
- The company's standard criteria for evaluating requests for expanded access
- The timeframe within which the company will acknowledge the request
- A link to the clinical trial registration information that the company posted to clinicaltrials.gov, with information about expanded access to the trial

Section 602 of the FDA Reauthorization Act ("FDARA"), which became law on August 18, 2017, increased the Act's requirement, requiring that sponsors post expanded access policies within 15 days of their studies' receipt of any of the following designations: breakthrough, fast track, or regenerative advanced therapy.

Meanwhile, more changes could be on the way in 2018. Senate bill S.204 (the "Right to Try" Act) passed the Senate on August 3, 2017. At the time of this writing, it's currently under consideration by the House. If passed in its current form, the new legislation would establish nationwide standards for expanded access to investigational medicines—standards similar to those already in force in 37 states. Also, it would make clinical trial sponsors exempt from certain provisions of the Federal Food, Drug, and Cosmetic Act, the Public Health Service Act, and other regulatory requirements. In addition, it would provide enhanced protection from liability.

Expanded access programs tend to be new ground for compliance professionals, who have traditionally focused on HCP-focused risks but are increasingly being pulled in to answer questions related to patient-focused risks as well.

In addition to complying with Section 3032 of the Act, compliance professionals have a role to play in evaluating their companies' ongoing compliance with the policies they set forth in this area and in understanding the effectiveness of their companies' controls to help prevent EAPs from being used as a tool to seed the market for drugs or biologics that have yet to be approved.

The Act also places a new emphasis on posting clinical trials to clinicaltrials.gov, an area where the industry has received low marks in the past. (A 2015 article in the New England Journal of Medicine, for example, put industry compliance in the range of 40 percent[10]). Possible fines for non-compliance with clinicaltrials.gov posting requirements are up to $10,000 per trial, per day.

Health care economic information

Section 3032 of the Act amends Section 502(a) of the Federal Food, Drug, and Cosmetic Act, clarifying and expanding guidance related to manufacturer dissemination of health care economic information (HCEI), which was last provided in Section 114 of the FDA Modernization Act of 1997 (FDAMA). Specifically, Section 3032:

- Expands the definition of HCEI to be "any analysis (including the clinical data, inputs, clinical or other assumptions, methods, results, and other components underlying or comprising the analysis) that identifies, measures, or describes the economic consequences, which may be based on the separate or aggregated clinical consequences of the represented health outcomes, of the use of a drug.

Such analysis may be comparative to the use of another drug, to another health care intervention, or to no intervention."

- Defines the audience eligible for communication as "a payor, formulary committee, or other similar entity with knowledge and expertise in the area of health care economic analysis."
- Requires that a "conspicuous and prominent statement" describing any material differences between the HCEI and the FDA-approved label must be included.

These changes are notable because they represent some of the first official guidance provided in this area in the 20 years since FDAMA passed. The industry has clamored for this guidance in the face of demands from the government and payers alike to migrate to outcomes-based pricing arrangements in value-based contracts.

To the extent that compliance professionals aren't already engaged with the teams responsible for managing HCEI studies, the data they generate, and the contracting provisions upon which they're based, this change in the regulatory landscape provides an opportunity to:

- Engage with the functions responsible for generating and executing ideas for HCEI research; understand how ideas are generated, triaged, reviewed, and approved; and understand whether this process occurs in a consistent and compliant manner that doesn't favor the scientific requests of one potential/actual customer over another (or the ideas of any customer over unmet and legitimate scientific and medical needs)
- Engage with the functions responsible for managing access to the data generated by these studies, to help ensure data is only used for its intended purposes in compliance with relevant laws and regulations
- Engage with the functions responsible for creating and negotiating contracts that may be based on this data; understand the terms and conditions of those contracts and whether they're creating unintended risk related to potential off-label promotion; and understand the fair market values of any services provided, as well as government price reporting laws and regulations

Taking decisive action in uncertain times

Regulatory uncertainty remains a fact of life. But in most cases, waiting for absolute certainty isn't a viable option. Instead, life sciences companies need to keep moving forward as planned, with deliberate linkage between:

- Regulatory strategy
- Business strategy
- Building infrastructure for governance, regulatory reporting, and risk management that scales and is flexible

Senior management will need to take decisive action while also paying close attention to emerging regulatory developments and staying as flexible as possible. The good news is that many of the changes life sciences companies are currently implementing make good sense from a business perspective—not just a regulatory perspective—and are worth doing no matter how the future unfolds.

Endnotes

1 "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff," October 2, 2014, US Food and Drug Administration, https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf.

2 "Postmarket Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff," December 28, 2016, US Food and Drug Administration, https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf.

3 AAMI TIR57: Principles for medical device security—Risk management, Association for the Advancement of Medical Instrumentation, http://www.aami.org/productspublications/ProductDetail.aspx?ItemNumber=3729.

4 "Managing Medical Device Security Risk," ***CIO Journal*** blog, Wall Street Journal, July 19, 2017, http://deloitte.wsj.com/cio/2017/07/19/managing-medical-device-security-risk/.

5 Notice: Transition Plan for the Medical Device Single Audit Program (MDSAP), December 4, 2015, Government of Canada, https://www.canada.ca/en/health-canada/services/drugs-health-products/medical-devices/activities/international/notice-transition-plan-medical-device-single-audit-program.html.

6 An in-depth look at the Act and its various provisions can be found at: https://www2.deloitte.com/us/en/pages/life-sciences-and-health-care/articles/twenty-first-century-cures-act-life-sciences-development.html.

7 "Submission to Congress: Food & Drug Administration Work Plan and Proposed Funding Allocations of FDA Innovation Account," June 6, 2017, US Department of Health and Human Services, Food and Drug Administration, https://www.fda.gov/downloads/RegulatoryInformation/LawsEnforcedbyFDA/SignificantAmendmentstotheFDCAct/21stCenturyCuresAct/UCM562852.pdf.

8 "Global HCP Transparency Study: Regulatory disclosure challenges and program guidance for life sciences companies," Deloitte Development LLC, 2013 https://www2.deloitte.com/us/en/pages/strategy/articles/global-hcp-transparency-study-regulatory-disclosure-challenges-life-sciences-consulting-services.html.

9 "Master Data Management: Building readiness for regulations," Deloitte Development LLC, 2017, https://www2.deloitte.com/us/en/pages/life-sciences-and-health-care/articles/master-data-management-for-product-information-pharmaceutical.html.

10 Monique L. Anderson, M.D., Karen Chiswell, Ph.D., et al., "Compliance with Results Reporting at ClinicalTrials.gov," ***New England Journal of Medicine***, 372:1031-1039, March 12, 2015, http://www.nejm.org/doi/full/10.1056/NEJMsa1409364#t=article.

Contacts

Leadership

Nicole Sandford
Regulatory & Operational Risk Leader
Partner | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
nsandford@deloitte.com

Bob Clarke
Advisory Life Sciences & Health Care Leader
Partner | Deloitte & Touche LLP
rclarke@deloitte.com

Jennifer Malatesta
Advisory Life Sciences Leader
Principal | Deloitte & Touche LLP
jemalatesta@deloitte.com

Chris Spoth
Executive Director, Center for Regulatory Strategy Americas
Managing Director | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
cspoth@deloitte.com

Authors

Kurt Conger
Managing Director
Deloitte Consulting LLP
kconger@deloitte.com

John Conrad
Principal | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
jconrad@deloitte.com

Mark DeWyngaert
Managing Director | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
mdwyngaert@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

Satyanarayana Patloori
Managing Director | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
spatloori@deloitte.com

Paul Silver
Principal | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
psilver@deloitte.com

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

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

The Center wishes to thank the following Deloitte professionals for their insights, contributions, and support to this report:
Regina Alvarado, Senior Manager | Deloitte Risk and Financial Advisory, Deloitte & Touche LLP
BJ D'Avella, Senior Manager | Deloitte Risk and Financial Advisory, Deloitte & Touche LLP
Lara Burkhart, Senior Manager | Deloitte Risk and Financial Advisory, Deloitte & Touche LLP
Clarissa Crain, Senior Manager | Deloitte Risk and Financial Advisory, Deloitte & Touche LLP
Leanne DiDomenico, Manager | Deloitte Risk and Financial Advisory, Deloitte & Touche LLP
Zach Dressander, Senior Marketing Specialist | Deloitte Services LLP
Stacy Hornaday, Manager | Deloitte Risk and Financial Advisory, Deloitte & Touche LLP
Ethan Joselow, Manager | Deloitte Risk and Financial Advisory, Deloitte & Touche LLP
Marcel Lissinna, Specialist Leader | Deloitte Consulting LLP
Ryan Press, Senior Marketing Specialist | Deloitte Services LLP
Nicole Schumacher, Senior Manager | Deloitte Risk and Financial Advisory, Deloitte & Touche LLP
Mutahar Shamsi, Specialist Leader | Deloitte Risk and Financial Advisory, Deloitte & Touche LLP
Nick Sikorski, Manager | Deloitte Risk and Financial Advisory, Deloitte & Touche LLP
Laura Skinner, Senior Manager | Deloitte Risk and Financial Advisory, Deloitte & Touche LLP

CENTER *for*
REGULATORY STRATEGY
AMERICAS

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.