Contents

Introduction 5
Drug pricing: more reporting, more oversight 6
Digital health technology and software as a medical device 12
Patient support/reimbursement support roles 18
Interaction with health care providers 11
M&A 25
Using artificial intelligence in compliance management 26
Additional regulations and trends 32
Staying ahead 35
Leadership 35
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 likely have a significant impact on the market and our clients’ businesses in 2020. 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 2020, 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 2020 and the regulatory changes it may bring. Please feel free to contact us with questions and feedback at CenterRegulatoryStrategyAmericas@deloitte.com.
Introduction

Life sciences companies are responsible for helping to improve the lives of millions of individuals and are necessarily held to a high standard of public trust. With such high stakes, regulators have made it clear that “paper compliance” is not enough and that companies are expected to maintain a comprehensive, real-time view of their compliance programs’ effectiveness.

Recent commentary by government officials highlights the need for companies to take a broader view of risk, to search for novel problems, and to take a close look at all aspects of company business to identify emerging risk activities. Likewise, recent enforcement activity related to prescription medications shows that federal agencies are integrating formerly isolated data and coordinating their activities in new ways. The changes to federal regulatory oversight are as much cultural as they are driven by process or technology.

To fulfill their own missions, life sciences companies should undergo a similar change toward achieving a holistic view of enterprise activities. Taking an enterprise-wide approach to compliance can mean that data, processes, and teams collaborate in new ways reaching far beyond program monitoring. Through an examination not only of technological and programmatic solutions, but also of company culture, today’s life sciences companies can be better prepared to meet the regulatory requirements and remain competitive in a fast-moving industry.

The theme for the 2020 regulatory outlook for life sciences is for companies to take a broader view of compliance so that these activities are part of a company’s overall business strategy. The 2020 regulatory outlook examines trends across the following topics:

- Combination products
- Distribution controls
- Interactions with health care providers (HCPs)
- Drug pricing
- Market access and patient engagement
- Medical device regulation
- Mergers and acquisitions
- Other regulations and trends

With compliance top of mind for all involved when a new product nears launch, a new system is brought online, or a new business relationship is explored, companies can be better equipped to do more than comply with regulation. Active compliance can also be a force to support the needs of your teams, and the process and technological tools they use, to be better integrated and aligned in your company’s mission.

We hope you find the insights provided by many of our Life Sciences leaders in the 2020 life sciences regulatory outlook a useful tool for as you navigate the evolving changes in the health care environment.
Drug pricing: More reporting, more oversight

As the price of health care has taken center stage in the policy debate, the pricing of pharmaceuticals has become one of the most talked-about areas of health policy today. The regulatory environment around drug pricing has always been complex, but has undergone significant growth in recent years, with no sign of slowing.

For life sciences companies, reporting and oversight of pricing and payment arrangements are growing areas of importance for regulatory compliance programs. Meanwhile, the push to value-based payment has begun to have a measurable effect on industry pricing practices. Despite the evolving state of the art, many companies continue to use existing accounting and finance functions that are distributed across various parts of the organization, which can lead to miscommunication and a lack of the coordinated strategy necessary to navigate the web of reporting requirements and their effects on pricing.

In response to these concerns, many companies are turning to integrated, enterprise-wide gross-to-net pricing models that rethink both systems and governance. With a comprehensive approach, life sciences companies may likely find that a strategic view of drug pricing compliance can pay big dividends.

**Price transparency requirements**

The movement toward transparency in health care has resulted in a number of state and federal entities requiring regular updates on various measures of drug pricing, with a variety of price increase thresholds determining when reporting is required. Across the country, nearly every state has become involved in regulating prescription drug pricing, with new laws mandating price reporting in an effort to improve price transparency, eliminate price gouging, and/or set the stage for inflation-based caps or other direct price controls.¹ All told, more than 50 transparency bills have been filed nationwide, with requirements varying greatly from state to state (figure 1).

State legislation around price transparency generally focuses on delivering specific commercial or statutory prices to the state in a defined manner and with defined timing. For life sciences companies, each new law will require documentation, processes, and controls to enable reliable and consistent price reporting and may trigger state oversight in certain circumstances.

Penalties for noncompliance with state transparency provisions are already mounting. In October 2019, Nevada fined 21 pharmaceutical companies a total of $17.4 million for failing to provide the state with explanations for recent price hikes on a set of diabetes drugs.² Nevada law allows the state to assess a $5,000 penalty for each day that a company is out of compliance with reporting requirements.

Oregon law requires drug manufacturers to report to the state’s Department of Consumer and Business Services information on prescription drugs where a drug’s wholesale acquisition cost is $100 or more for a one-month supply (or for a course of treatment lasting less than one month), and when the drug’s wholesale acquisition cost (WAC) increased by 10 percent or more over the previous year. Where reporting is required, a manufacturer must also report the factors behind the price increase; research and development costs for the drug; direct costs to manufacture, distribute, and market the drug; previous-year profits for the drug; and the 10 highest prices paid for the drug during the previous year in any country other than the United States.

**Implications of new transparency laws**

New price transparency requirements present new challenges. In addition to penalties for noncompliance, public disclosure of information can lead to potential inconsistent public information or messaging and the exposure of trade secrets, allowing for sophisticated analysis by competitors, the media, and special interest groups. For these reasons, it is essential for pharmaceutical manufacturers and distributors to stay apprised of regulatory changes and to carefully manage changes to business processes that could affect reporting.

**How to prepare**

In response to the challenges, we recommend that affected companies undergo a thorough, regular applicability review of state price transparency regulations and seek out leading industry practices for maintaining compliance.
## Life sciences regulatory outlook 2020

### Drug pricing: More reporting, more oversight

<table>
<thead>
<tr>
<th>STATE</th>
<th>CA</th>
<th>CO</th>
<th>CT</th>
<th>LA</th>
<th>MD</th>
<th>ME</th>
<th>NV</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Report date and frequency</strong></td>
<td>New Drug Notification within 3 days after first order date and New Drug Report within 30 days of New Drug Notification; Price Increase Notification is 60 days in advance of planned WAC increase that exceeds trigger and Report is Quarterly</td>
<td>On an ongoing basis when conducting business with the provider</td>
<td>New Drug Notification within 60 days of receiving an action date from the FDA regarding an NDA or BLA application; Price Increase Notification and Report may begin on or before May 1, 2020</td>
<td>WAC reporting is the First date of each Quarter</td>
<td>Establishes a Prescription Drug Affordability Board; The Board may request information from the manufacturer to the extent there is no publicly available information to conduct their cost review</td>
<td>LD 1499 Establishes a Prescription Drug Affordability Board; LD 1162 Price Increase notification and new drug notification for any drug launched that has a WAC greater than Medicare Part D threshold</td>
<td>Price Increase Report and justification on or before April 1 of each year</td>
</tr>
<tr>
<td><strong>Special requirements</strong></td>
<td>$&gt;40 WAC, 16% WAC increase thresholds current +2 prior calendar years; additional information for newly-launched or recently acquired products</td>
<td>Product is marketed in Colorado</td>
<td>$50% WAC increase in past 3 years or &gt;20% increase in prior 12 months; &gt;$60 for 30 day supply</td>
<td>Product is marketed in Louisiana</td>
<td>N/A</td>
<td>WAC of brand-name drug by more than 20% per pricing unit; Drug costs at least $10 per pricing unit by more than 20% per pricing unit</td>
<td>Essential diabetes drugs only as determined annually by Nevada Department of Health and Human Services</td>
</tr>
</tbody>
</table>

### REPORTING CONSIDERATIONS

| WAC price | X | X | X | X | X | X | X |
| New drug notification | X | X | X | X |
| Threshold-based reporting | X | X | X |
| R&D, sales, and/or marketing costs | X | X | X |
| Contextual information (justifications, factors, etc) | X | X | X |
| International price details | X | X | X |
| Reporting upon request | X | X | X |
| Penalties | X | X | X | X |

---

**Figure 1.** A sample of enacted state price transparency laws
With a firm understanding of the regulatory landscape—and mechanisms for assessing changes—the next step is to develop clear standard operating procedures for state price transparency requirements to confirm data is captured and reported in a way that meets the growing permutations of reporting structures from state to state. These documents should identify the functional groups within each organization that are responsible for completing the steps required for compliant reporting. Also, reporting methodologies should specify the type, content, frequency, and recipients for each required report.

In some cases, legislation might not be explicit in the required timing or manner of reporting. In these instances, manufacturers have begun to develop reasonable assumptions to guide their activities related to compliance with specific state legislation. As with the reasonable assumptions manufacturers have developed in response to other government agency reporting, legal counsel will likely need to drive development of the assumptions in order to determine what will make sense for the business given the intent of the legislation.

**Innovations in price contracting**

Like the broader shift from volume to value in health care, the concept of relating payment for a drug to its value has taken hold with public and commercial payers alike. Among both life sciences companies and health care payers, there is a burgeoning interest in accelerating the execution of value-based contracts (VBCs). A 2017 survey of payers and pharmaceutical manufacturers found that nearly all respondents described VBCs as offering positive value for their organizations, and the volume of VBCs is expected to grow by two to three times over the next few years.³

**Building the capabilities**

Real-world evidence is at the center of any efficient and effective VBC arrangements. The Deloitte Center for Health Solutions’ 2018 Real-world Evidence Benchmarking Survey found that 90 percent of responding life sciences companies are establishing or investing in real-world evidence capabilities for use across the product life cycle, though only about half of those companies said their capabilities are mature enough to meet today’s challenges.⁴

Despite the interest, many organizations do not have the infrastructure needed to support VBCs across their market offerings. Infrastructure challenges include having the systems to collect, aggregate, and store reporting data, as well as contract administration that can effectively oversee complex relationships with payers. Also, once a VBC is in place, advanced analytics are needed to ensure that the value proposition agreed on between payer and manufacturer is realized in practice.

VBCs are based on the premise that a drug that is properly administered in an optimal care environment will deliver value for all concerned. Thus, all parties to the contract should face some risk or benefit from outcomes. A fair contract includes agreement on the patient population for inclusion and on outcomes that can be objectively measured and are reproducible.

Since VBCs rely on clinical outcomes, pharmaceuticals sold under VBC arrangements require additional patient education and support to maximize regimen adherence. And even then, population health risks are difficult to quantify, patient adherence can be challenging, and prescribing or administration errors on the part of the health care provider remain a possibility.
Compliance and regulatory considerations

While value-based payment arrangements are themselves complex, they also expose life sciences companies to patient privacy and anti-kickback issues, as well as other government price reporting compliance considerations.

Existing laws around fraud and abuse, such as the Anti-Kickback Statute, do not address VBC arrangements. Recent proposed rulemaking adds safe harbors for a range of value-based payment arrangements in health care, but does not address pharmaceuticals. While pharmaceutical-specific VBC regulation is under consideration, the Office of the Inspector General’s (OIG) rule states explicitly that “These kinds of manufacturer arrangements raise different program integrity issues from those addressed in this rulemaking and would likely require different safeguards.” As such, there are no contract terms that can protect against perceptions that clinical decision-making is influenced by a VBC. To achieve compliance in a complex and ambiguous regulatory environment, life sciences companies will need to have a deep understanding of the VBC landscape, as well as benchmark arrangements other drug companies have entered into, and work closely with their counsel.

In addition, current government price reporting requirements do not address VBC arrangements and make certain VBC arrangements challenging for manufacturers to enter into. For example, patient outcome–based price concessions to commercial payers on brand-name drugs can set a low best price (BP) for a drug, even if only one commercial unit of a drug were to fail a patient-outcome criterion and thereby increase the Medicaid Drug Rebate Program (MDRP) rebate amount for all Medicaid units, even if no Medicaid unit were to fail the metric. There also may be operational and compliant BP reporting issues with offering outcome-based pricing based on the long-term durability of a drug. Further, there have been challenges with certain payment over time VBC arrangements due to the impact on average manufacturer price (AMP) and associated inflation penalty as part of the MDRP. Finally, VBC arrangements may be structured as bundles, creating operational challenges for drug companies—any type of bundling will need to be unbundled for statutory price calculations—and the more complex the bundling (temporal, products, entities, etc.) the greater the potential impact on overall operations.

How to prepare

Life sciences companies should consider adopting a concerted approach for meeting the challenges and opportunities of VBC arrangements. Considerations include:

- **Scenario analysis.** A company should develop a forecasting and scenario analysis framework for potential VBCs that include the products in its portfolios. Findings from the scenario analysis should emphasize financial impacts and be shared across a cross-functional team—with any offsets from government programs being considered in the overall impact to the business. Of course, all scenarios need to be driven by reasonable assumptions, and those assumptions should be discussed with internal or external legal counsel so they are compliant with applicable regulations and guidance.

- **Prepare for rapid implementation.** Every unique arrangement will have its own set of impacts on a manufacturer’s present and future business. For example, a new contract arrangement will have operational considerations and may require updates to current processes, documentation, and systems. Given the complex relationship between public and private drug pricing, controls should be in place to assess whether commercial decisions might have secondary effects on government programs. In all, it is advisable to develop an operational roadmap and process flows that outline operational changes whenever a new contracting approach is implemented.

- **Have the players in place.** Life sciences companies will need to assign responsibilities and develop processes to support the ongoing monitoring of novel contracting strategies. It will be important to be able to communicate the impacts that VBC arrangements can have across pricing strategies. Likewise, it takes a diverse set of knowledge and skills to operationalize VBCs while remaining compliant. This will require a dedicated team of legal, IT, commercial, and clinical professionals, each with their own skill set, but each also understanding the full range of implications related to VBCs. It may also take involvement from Government Affairs to assist in helping government agencies to understand the limitations of current laws and potential solutions that represent a win-win approach.
340B program integrity
Although new 340B legislation appears unlikely in the near term, regulators continue to focus on 340B as a target for program integrity initiatives, with manufacturers often at the center of attention.

New reporting systems
In 2019, the Health Resource and Services Administration (HRSA) rolled out a new secure pricing component of the Office of Pharmacy Affairs Information System (OPAIS), 7 which provides covered-entity and manufacturer-authorized users with access to 340B ceiling prices. The new system gives covered entities a clear breakdown of how a drug’s AMP relates to a ceiling price, as well as a breakdown of the subsequent rebate they are entitled to receive. In all instances, the AMP calculation drives the level of rebate, meaning that a manufacturer’s average price is a strategic decision.

The 340B Ceiling Price and Manufacturer Civil Monetary Penalties Final Rule 8 now requires manufacturers to true-up Provisional 340B Ceiling Prices for new products and refund overcharges to covered entities within 120 days of overcharge determination. These regulations address civil monetary penalties that can be imposed on manufacturers for “knowingly and intentionally” overcharging 340B covered entities at a price above the 340B ceiling price.

Manufacturers face both compliance risk and reputational risk with their 340B customers and within the industry if they do not adhere to 340B program requirements. Manufacturers should take precautions to mitigate such risk and prepare for the HRSA audits that are now part of the agency’s program integrity priorities.
Strategic opportunities in drug pricing

Many parts of a life sciences organization see pricing compliance as a barrier to surmount, or as an added complication in their pricing strategies. The reporting requirements are complex, and unlike other aspects of compliance, often require close coordination with commercial, internal audit, and legal to confirm that reporting occurs both in accordance with the law, and to the maximum advantage of the company.

With so many factors in play, gross-to-net forecasting and accruals are a significant challenge facing many pharmaceutical companies today. Factors such as product portfolio changes, pricing and contracting strategy changes, and uncertainty with downstream data make it difficult for manufacturers to manage their gross-to-net process. To take a strategic approach, drug manufacturers should undergo a continual assessment of their financial models.

In the end, effectively and efficiently navigating the intricacies of drug pricing compliance and optimization requires a highly integrated management structure, coupled with a unified approach to reporting. Establishing these capabilities can not only help a company succeed in drug pricing, it can also create new synergies between Compliance and other business units that yield company-wide benefits.
Digital health technology and software as a medical device

Across many industries, technological innovations are moving faster than the speed of regulation. In many cases, regulation falls behind when new products challenge the established taxonomies of products that the regulator has traditionally overseen.

In the medical device industry, this change has been especially notable in software-enabled products—devices that generate, analyze, and transmit health data via the Internet of Medical Things (IoMT). The IoMT market is among the fastest-growing medical sectors in the world. By 2022, the IoMT market is expected to top $158 billion globally.¹ Medical device manufacturers recently estimated that almost half (48 percent) of their products are data-generating connected medical devices. Over the next five years, manufacturers expect that percentage will jump to 68 percent, according to a 2018 report from Deloitte that explored connected medical devices.

The future of health is one where digital health technology allows for real-time monitoring of complex medical conditions, while the collection of data informs medical research, clinical practice, and device design improvements. As this connected future takes shape, so do concerns from regulators and the public about cybersecurity. In addition, the incorporation of digital health technology draws new entrants such as software and consumer product–oriented companies, often without a strong background in medical device safety and regulation. The combination of new applications and new players with a nonmedical background presents a heightened level of risk to the development and marketing of digital health technology.

Digital health technology in today’s risk environment

The advent of Software as a Medical Device (SaMD) provides a clear example of new regulatory and post-approval concerns. SaMD attracts software companies that are often accustomed to far faster product cycles and minimal government oversight. These entrants do not necessarily know the full range of regulatory and product safety risks, or how to work with other partners, such as hospitals, payers, and traditional medical device manufacturers that may deploy their software or use it as an interface to other systems. Without experience working with regulators, these companies are unlikely to have developed the controls and oversight that are considered standard compliance guardrails by more traditional manufacturers, and many have already become caught up in regulatory and reputational risk.

However, even traditional device and pharmaceutical manufacturers may face challenges and issues complying with the unique risks associated with SaMD products. Standard approaches to risk mitigation, which have traditionally focused on the device itself, are not adequate to address risks that extend beyond the device; for example, vulnerabilities that exist in the infrastructure on which the device sits and on which it relies to communicate information to and from the user.

Also, the risks associated with any medical device only grow once it is approved and in the field. In the case of SaMD, such device’s software will interact with a number of stakeholders, including patients, caregivers, practitioners, payers, Internet service providers, and third-party contractors, each adding to the marginal risk associated with the product.

SaMD product developers should look closely at their approach to adverse event reporting and patient safety and be prepared for ongoing monitoring by regulators. Without a coherent strategy, even some manufacturers of traditional devices have experienced problems in this space and, as a result, have faced civil monetary penalties, consent decrees, and court injunctions. These compliance issues are only exacerbated for SaMD manufacturers. Beyond the more standard regulatory concerns related to medical devices, SaMD products should address the issues of privacy and protected health information and should be prepared to meet the standards established such as those in the US Health Insurance Portability and Accountability Act (HIPAA) and the European Union’s General Data Protection Regulation (GDPR).

Thinking about SaMD risk

There are five broad categories of risk in SaMD development and marketing, each with its own considerations that are unique to SaMD products.

• Design control. Design approval is more challenging with software-based medical devices, because there is a higher risk of defects or functionality discrepancies surfacing later in the production process and of software bugs being discovered during analysis.
• **Risk management.** With the complex nature of software development, risk management should be performed with a greater level of detail both in the design stage and throughout the device’s life cycle.

• **Cybersecurity and data privacy.** Cybersecurity and data privacy concerns can pop up anytime and anywhere in a device’s life cycle and may involve systems not under the manufacturer’s direct control (e.g., a hospital network). Security issues do not have a grace period. They are a priority that should be constantly assessed for risk and promptly mitigated.

• **Postmarket surveillance and end-of-life (EOL).** The tighter connection of SaMD products to patients and HCPs enables the collection of vast amounts of data that may be used for market/user analysis and product improvement. However, it is also another input for potential Adverse Event/Medical Device.

• **Compliance risk.** For any manufacturer considering the distribution of tablets, phones, or watches in association with their respective SaMD or planning to distribute information about products or diseases via the applications that might be considered SaMDs, considerable regulatory and legal risks exist that need to be vetted and mitigated throughout the life cycle of such products.

Reporting medical device regulation (MDR) information, which should be processed and acted upon in a timely manner, may strain current internal systems. Further, the need to enable, monitor, update, and even withdraw SaMD products from the marketplace, after they leave the direct control of the manufacturer, provides additional compliance challenges.

---

**An overview of the US and EU regulatory landscapes**

While not exhaustive in terms of global scope, the regulatory processes in the United States and European Union provide a good general overview of how regulators are treating SaMD and medical device cybersecurity.

**FDA guidance on cybersecurity**

Since the US Food & Drug Administration (FDA) released its [initial guidance](https://www.fda.gov) in 2014 on premarket submissions for management of cybersecurity in medical devices, the industry and the regulatory environment has advanced. Over the past five years, the FDA has issued new guidance on pre- and postmarket submissions for interoperable medical devices. At the end of 2016, the FDA finalized its [guidance on postmarket management of cybersecurity in medical devices](https://www.fda.gov), and on October 18, 2018, the FDA published a [draft guidance update](https://www.fda.gov) for “Content of Premarket Submissions for Management of Cybersecurity in Medical Devices.” The draft guidance update enhances recommendations to the industry regarding cybersecurity device design, labeling, and the documentation that the FDA recommends be included in premarket submissions for devices with cybersecurity risk. Manufacturers must demonstrate an understanding of the cyber risks inherent to the systems and devices and how to manage those risks throughout the life cycle.

Since the initial premarket guidance, many industry stakeholders have struggled with understanding the level of analysis the FDA expects on connected medical devices and what documentation to include in submissions. Through the guidance update, the FDA has clarified specific considerations for premarket submission documentation and stressed the importance of
risk-based rationales provided as part of submissions need to

While the 2018 guidance is still in draft form and will not formally replace the 2014 guidance until it is finalized, the latest version of the guidance includes a few new additions and enhancements to earlier recommendations of which manufacturers should be aware. Each of these changes could be covered in great depth; however, for the purposes of this overview, our discussion focuses on how the FDA is enforcing the draft guidance.

Regarding the tiering approach of medical devices based on cybersecurity risk, the FDA is looking for holistic use cases that link threat modeling to risk assessment to design decisions and evaluation of control effectiveness. As usual when interacting with the FDA, the expectation is that each of these elements is documented, clear, and traceable. Once the device is tiered, the expectation is that this tiering would result in a set of design controls for cybersecurity. With the guidance update, the FDA introduced a set of design controls for cybersecurity that should be adhered to. Regardless of the device, the FDA is focused on understanding how the device manufacturer and medical device are conforming to these design controls. There is a particular focus on certain controls that are more important from a risk perspective, such as mutual authentication.

The updated guidance introduces the concept of establishing and monitoring a cybersecurity bill of materials (CBOM) for security vulnerabilities. Based on recent discussions with regulators, the final guidance will probably reference a software bill of materials (SBoM) rather than a full CBoM that includes hardware components that are or could become susceptible to cybersecurity vulnerabilities. Within submissions, the FDA is expecting the manufacturer to include a SBoM, known vulnerabilities with the software components, remediation that has taken place (e.g., patching), and testing that verifies the effectiveness of the remediation.

The previous version of the FDA’s premarket guidance did not clearly define how to calculate the likelihood of a vulnerability being exploited, which resulted in varied calculations based on probability and exploitability across the industry. Through this guidance update, the FDA clarified that security risk analysis and risk-based rationales provided as part of submissions need to leverage an analysis of exploitability to describe likelihood instead of probability. An expectation is that security assessment (e.g., threat modeling, architecture review, testing) incorporates exploitability-based vulnerability analysis. The FDA is looking for a comprehensive traceability matrix that includes identified risks, compensating controls, residual risk, and testing that verifies the adequacy of control measures.

Regarding labeling, several FDA regulations discuss labeling requirements for medical devices (e.g., Sections 502(a)(1), 502(f), and 201(n) of the Federal Food, Drug, and Cosmetic Act (FD&C Act); 21 CFR 1.21, 801.5, and 801.9(c)). Through the updated draft guidance, the FDA suggests that for devices with cybersecurity risks, informing end users of relevant security information may be an effective way to comply with labeling requirements and an important part of quality system regulation (QSR) design controls to help mitigate cybersecurity risks and assist with the continued safety and effectiveness of the device. In submission documentation, the FDA is looking for manufacturers to provide detailed cybersecurity information (e.g., a summary of security safeguards, customer requirements and expectations, SBoM, and design documents such as architecture diagrams and data flows).

Overall, these enhancements have introduced a far more actionable guidance for medical device manufacturers and have raised the bar on what is expected of them before they can sell their devices in the United States. In addition, this guidance is being enforced by the FDA, which is holding the device manufacturers accountable. At times, this enforcement may result in devices not being approved for cybersecurity reasons. This is a big step for the medical device industry and should result in safer devices hitting the market.

Along with the draft guidance, the FDA has established a Precertification Pilot Program to precertify SaMD products under certain circumstances. A range of companies, some of which are not traditionally medical in nature, have been selected as participants. The goal of the program is to bring companies that are new to the medical device industry into the agency’s regulatory framework and 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.”
European Union guidance on cybersecurity

Cybersecurity policy for medical devices in the European Union is part of a larger recent effort to enhance data protections, which includes the implementation of the General Data Protection Regulation (GDPR), the granting of permanent status to the European Union Agency for Network and Information Security (ENISA) as an oversight body, and the upcoming implementation of the Medical Device Regulation (MDR) and In-vitro Diagnostic Regulation (IVDR).

GDPR

When the GDPR took effect on May 25, 2018, it superseded the European Data Protection Directive. Unlike the earlier directive, the GDPR is a legally binding regulation with significant penalties for violation.

ENISA

ENISA maintains a set of Baseline Security Recommendations for the Internet of Things (IoT) that covers transportation, energy, and mobile payments in addition to health care. The recommendations are intended to promote broad-based security principles across the EU data infrastructure, as well as provide a practical framework for IoT marketers to comply with the GDPR. Where medical device security is concerned, the ENISA IoT recommendations generally follow the FDA guidance.

MDR and IVDR

The new European MDR and IVDR are comprehensive regulations designed to harmonize and simplify how medical devices are approved and monitored for compliance across the European Union. While many of the MDR and IVDR rules are about safety, efficacy, and reporting, there are a few provisions where cybersecurity comes into play. One example is where the MDR’s safety and performance requirements call for devices to be “designed and manufactured in such a way as to remove or reduce as far as possible . . . risks associated with the possible negative interaction between software and the IT environment within which it operates and interacts.” With the MDR taking effect on May 26, 2020, it is important to be aware of its implications to security, since the MDR will be the standard by which rules are enforced, while other documentation, such as the ENISA IoT recommendations, provide the design principles. However, the requirements under EU MDR/IVDR go far beyond cybersecurity.

Broadly speaking, the MDR aims to create a new and improved landscape for the medical device industry, with the following new guidelines:

- All medical devices will have to undergo an independent assessment of safety and performance before they can be marketed in the European Union.
- Products that were not considered devices under the earlier...
Medical Device Directive will now be classified as medical devices. In addition, under both MDR and IVDR, the classification of some devices will change to higher risk categories.

- The new rules require a more comprehensive clinical assessment of safety for higher-risk devices, which must be documented in technical file submissions.
- The EU MDR will place further responsibilities on “notified bodies”—those independent third parties that perform conformity assessments for medium- and high-risk devices. The notified bodies will be subject to heightened scrutiny from competent authorities and will need to be designated under the EU MDR, with the process of designation coordinated at a European level.¹
- Postmarket clinical follow-up will be more extensive, further complicated by novel channels, such as social media and SaMD, and will require more sophisticated techniques and more effort.
- Many device categories will now require a unique device identifier (UDI)/implant card.
- The new European Database on Medical Devices (EUDAMED) system will require much more information from manufacturers. Among other things, it is intended to contain information on companies, UDIs and devices, notified bodies and certificates, vigilance, clinical investigations, performance studies, and market surveillance, as well as serving as a system for registration, collaboration, and notification and as a publicly available dissemination system. While the implementation of EUDAMED was recently delayed by the European Commission, it still represents a significant compliance challenge that should not be ignored.
- Enhanced responsibilities for economic operators (e.g., manufacturers, distributors, suppliers, subcontractors, EU-authorized representatives) will require revised governance models.
- There will be greater transparency of information on the benefits for patients and residual risks; also, a thorough assessment of the overall risk/benefit ratio will be necessary.
- There will be clearer rules in place to enable standardization and support simpler and less complex trading between EU member states; those that do not comply will be penalized.
- The new rules support patient-oriented innovation and take particular account of the specific needs of the many small and medium-sized manufacturers in this sector.

Beyond the EU-level directives, many member states have published their own guidance and rulemaking around medical device cybersecurity.
Quality management system (QMS) changes

In light of new regulatory requirements and changing industry practices, companies should undergo a thorough review of their QMS approach to ensure that the right procedures are in place for today’s needs. For example, UDIs will need to be appropriately across different jurisdictions, and more complex supply chains require quality management to reach further into vendors' and partners' own quality protocols. As part of their review, companies should be aware of the following:

• Procedures around device risk analysis and classification should be revised to address the new decision processes.

• Postmarket analysis and product design feedback processes—and the procedures that govern them—will need to be revised to address the new data channels.

• Procedures related to product design, manufacturing, and distribution and postmarket need to be updated to ensure traceability in accordance with UDI requirements under EU MDR/IVDR.

• Procedures should be revised to ensure that expanded responsibilities for vendor oversight across the supply chain are addressed, including contacts, quality agreements, and vendors and service providers that audit processes.

• Procedures around problem tracking and reporting, as well as the systems used to perform those functions and maintain the associated data, will require extensive and fundamental revision in order to meet the reporting requirements of the new EUDAMED.

New regulation in 2020, and an evolving ecosystem of technologies and security vulnerabilities, means that cybersecurity will demand more attention than ever before.

With so much change in play, all stakeholders should be sure to maintain a balance between transforming patient care and the associated risks inherent to this new world. The future of health is interconnected and patient-centered, but at its foundation, the future of health needs to be secure.

Patient and reimbursement support roles

In an effort to improve patient access to prescribed products, many manufacturers use field-based personnel to provide certain reimbursement and patient support services to HCPs, their staff, and patients. Generally, patient and reimbursement support services are carried out by nonpromotional, field-based personnel who seek to support the reimbursement of, and education about, a manufacturer’s products to help patients access the medicines they need.

Examples of patient and reimbursement support roles include:

- **Field reimbursement personnel** interacting with HCPs and their staff to support patient reimbursement, coverage, and access to prescribed products
- **Patient assistance coordinators** interacting with patients, focusing on unbranded disease-state education
- **Clinical nurse educators** interacting with patients, focusing on education related to the administration and use of a manufacturer’s product(s)

What are the regulatory risks?

Regulatory risks to consider include:

- **Anti-Kickback Statute** – Prohibits offering a prescriber anything of value to induce, reward, or encourage the recommending or prescribing of a product that is reimbursed by the government
- **False Claims Act** – Prohibits inducing or encouraging an individual to make false or fraudulent claims for reimbursement of a prescribed product from the federal government
- **HIPAA and other privacy laws** – Impose strict limitations on the use and disclosure of patient information, including protected health information (PHI)
- **FDA statute and regulations** – Regulate product advertising and promotion; promotional materials may include only those claims about a product that are consistent with that product’s labeling. Activities that do not have documented controls, parameters, or other guidance can run afoul of various FDA regulations.

Recent allegations include:

- Allegations that a manufacturer provided HCPs with access to field reimbursement personnel and services as an incentive to prescribe the manufacturer’s products
- Allegations that a manufacturer used clinical nurse educators to ensure that prescriptions were refilled

Key considerations

Manufacturers should consider the following questions and related actions when evaluating their patient and reimbursement support roles:

**What level of support do the patient and reimbursement support roles provide to HCPs and patients?**

- Create an inventory of all activities the roles provide to HCPs and patients
- Evaluate the totality of support provided by the roles to ensure that the support does not constitute substantial independent value
- Evaluate the support provided by the roles to ensure controls are in place to guard against white coat marketing
- Limit interactions between the roles and HCPs to only those HCPs that are likely to prescribe the product for on-label uses
- Conduct regular auditing and monitoring of the roles’ activities to review compliance with company policies and guidelines

**Could the patient or reimbursement support roles be perceived as a “sales” role?**

- Review the internal reporting structure of the roles to ensure the roles are not perceived as sales roles
- Ensure that compensation provided to the roles is not tied to prescription volume
- Review training content to ensure the content provided to the roles...
Life sciences regulatory outlook 2020 | Patient and reimbursement support roles

is different than the training provided to sales and marketing personnel

• Review materials and communications to ensure the content is transparent about the remit of the roles and not promotional in nature
• Make the roles available to all HCPs and patients, regardless of HCP prescription activity
• Limit pre-prescription interactions between the roles and patients

What controls are in place to protect patient privacy?

• Implement processes to limit situations in which the roles may come across patient information
• Prohibit the roles from collecting and retaining patient information

What guidelines or “rules of the road” exist to guide interactions between patient and reimbursement support roles and other field-based roles (e.g., sales representatives, field medical personnel)?

• Document clearly defined roles and responsibilities for each field-based role
• Implement clear, written guidelines on the do's and don'ts for communications and interactions between patient and reimbursement support roles and other field-based roles that allow patient or reimbursement support roles to remain independent from commercial influence.

Example considerations include:
– Limiting communications to logistical discussions and background discussions about HCPs
– Prohibiting discussions related to HCP prescribing habits or sales messaging or strategy
– Documenting a clear point of transition in the sales cycle (with some overlap as needed) where responsibilities are transitioned from sales colleagues to patient or reimbursement support roles

Moving forward

The considerations noted in this document are just a starting point for manufacturers to consider in reducing the risks associated with patient and reimbursement support roles. Manufacturers should continue to assess and enhance their relevant processes and controls to help ensure compliance with the evolving regulatory landscape and to meet the increased government scrutiny on these roles.

Let’s talk

BJ D’Avella
Senior manager
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
bdavella@deloitte.com

Elaina Filauro McEwan
Senior manager
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
efilauro@deloitte.com

Russell Rose
Senior manager
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
rusrose@deloitte.com
Interaction with health care providers

Pharmaceutical, biotech, and medical device companies routinely interact with external HCPs, either through contractual arrangements like paying a standard fee, or noncontractual arrangements such as providing lunches to doctors’ offices. These 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. Globally, HCP contracting is subject to the US Foreign Corrupt Practices Act (FCPA) and a number of other codes and regulations, such as France’s Loi Bertrand Sunshine Act, the UK Bribery Act, and the Medicines Australia Code of Conduct.

This issue is not new, it is not going away anytime soon, and the scrutiny is intensifying. The US Department of Justice (DOJ) recently made clear in updated guidance to its prosecutors that corporate compliance programs must take a closer look at their firm’s risk profiles than ever before. With the knowledge that prosecutors and regulators are setting a high standard of oversight, a culture of prevention—as well as detection and correction—should be front of mind for compliance programs. It is, therefore, essential for companies to manage and execute HCP engagements as efficiently and effectively as possible, with appropriate controls and documentation.

The state of the art in HCP engagement compliance is evolving alongside regulator guidelines. In the near term, many life sciences companies will need to revisit existing business processes and assess where new technologies can assist with risk mitigation while increasing productivity. With so much change underway, a formal process and infrastructure that addresses end-to-end business, functional, and compliance requirements across the HCP engagement continuum has become central to preventing, identifying, and remediating compliance concerns.

People and process first

In response to public pressures, processes are changing. A Deloitte survey of life sciences companies’ HCP engagement compliance programs found that most responding manufacturers have recently switched to an annual review process of their engagements, moving away from earlier approaches consisting of review upon contract renewal, ad hoc reviews, or updates as organizations became aware of changes.

These changes in program expectations are leading many toward technological solutions, but the process of overhauling a company’s compliance and audit functions cannot be rushed. The implementation of new technologies should only come after a careful review of a company’s vision and strategy and a rethinking of the roles that people play, as well as the processes they operate under.

Technology is only as valuable as a company’s governance and operating rules allow. For that reason, technological solutions should come at the end of a number of other considerations. The Deloitte survey found that many key governance functions for HCP compliance are divided between different business units, without a clear chain of command or identification of responsibility. Before any technological solution, life sciences companies should address executive sponsorship, create a clear delegation of responsibilities, and make a commitment to continuous training. After governance comes operations. Rules around data acquisition, maintenance, and
handling will provide the structure needed for successful automation. Technology can only succeed once the right structure and rules are established.

**Where technology comes into play**

Even with the perfect workflows, policies, and procedures, 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.

Once the right policies and procedures are in place, today’s life sciences companies should consider leveraging technology solutions to automate activities and controls and to assist with ongoing compliance monitoring. With major advances in automation and artificial intelligence (AI), 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.

As a general matter, to implement an enterprise-wide system that can execute activities and compliance controls across the HCP engagement continuum, life sciences companies should:

- Clearly define business, functional, compliance, and process flows prior to configuring the off-the-shelf system
- Identify and define integration requirements for internal and external systems that will provide data and should interface with the HCP engagement continuum
- Create broad test plans, scenarios, and scripts to confirm that configured end-to-end functionality satisfies specified requirements
- Provide dedicated project and program management oversight to coordinate implementation activities, timelines, and budget tasks
- Create required system development life cycle artifacts
- Consider change management and training requirements for affected business functions

With the ground rules established, life sciences companies can begin to assess the array of technological solutions to find the best fit for their programs.

**Using off-the shelf technology to automate the HCP engagement monitoring process**

The Deloitte survey of HCP engagement compliance programs found that over half of responding life sciences companies indicated that they are planning to implement a system to automate the process for managing HCP engagements. Additionally, over half the companies surveyed indicated that they prefer to implement an off-the-shelf software-as-a-service (SaaS) application to automate processes that comprise the HCP engagement continuum.

Many of the workflows associated with HCP engagement monitoring readily lend themselves to the automation found in SaaS packages, 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, removing 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.

Making the most of cognitive technologies
At present, most monitoring platforms that use cognitive technologies are in a process of advancing from being able to accurately categorize and prioritize issues that arise in complex data to platforms that can implement continuous improvements through machine learning that requires less human input. Even as cognitive technology is still maturing, life sciences companies are finding that they can already significantly improve their efficiency and effectiveness in managing HCP interactions, while at the same time reducing their risk exposure. In addition, 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.

HCP contract review
Cognitive technology, such as AI, has made it possible to create an automated process for reviewing and approving HCP contracts with little or no human involvement. As a practical matter, HCP contract review often deploys three types of technology:

1. Natural language processing analyzes terms and conditions.
2. Software bots apply rules and AI to evaluate contracts and qualifications using the same criteria as humans, replacing or augmenting human judgment.
3. Machine learning enables the system to learn from experience and get smarter over time.

Current systems with cognitive technologies can accurately and confidently make “approve” or “reject” decisions for more than 70 percent of contracts. In the minority of cases where the system is unsure, it automatically routes the contract to a human specialist, with questionable elements highlighted to make the manual decision-making process much faster and easier.

A recent survey of compliance professionals conducted by the Deloitte Center for Health Solutions relays the experience of a large pharmaceutical company that has devoted considerable effort to retrospective review of emails as part of their risk monitoring. Since the company deployed a natural language tool for initial email screening, the number of emails that compliance officers needed to review went from 2,500 to 20.7

About public reporting
The Centers for Medicare and Medicaid Services’ (CMS) Open Payments database has become a rich resource for government regulators. The HHS OIG and DOJ have stated that they will combine Open Payments data with other available data sets to pursue anti-kickback investigations. Open Payments data is being used by others aside from federal regulators. 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 the extensive 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. A secondary benefit to consider is that regulatory reporting is driven by the same data and analytics for spend analysis and commercial considerations, presenting an opportunity to improve a company’s own tools for leveraging data.

Companies are expected to be proactive on transparency analytics and compliance
The DOJ makes clear that companies should be proactive in assessing and remediating their compliance risks in general and has placed a particular emphasis on HCP engagements. Even before the new guidance to prosecutors, in 2016, Laura M. Kidd Cordova, Assistant Chief, Criminal Division, Fraud Section, DOJ, made this point by stating, “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.” 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.”9
With so much government and public scrutiny on Open Payments, at a minimum, life sciences manufacturers should be able to correlate supporting data and/or supporting documents to help:

• Detect compliance patterns and take corrective actions before they become issues
• Explain any identified anomalies
• Use these findings to enhance compliance and HCP engagement programs

Given today’s data-driven business environment—with its unprecedented volume and accessibility of internal and third-party data—life sciences companies should heed regulators’ statements that the Open Payments system is a valuable tool in their ongoing compliance efforts.

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 need processes, policies, and procedures to ensure the right transparency data is 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 or 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 and implemented technology.

A good first step is establishing a continuous risk assessment and monitoring program. An effective risk assessment and mitigation planning program can serve as the backbone for all other compliance efforts and provide evidence that the company is routinely identifying risks, areas for improvements in controls, and other mitigation activities to create a cycle of continuous improvement that becomes part of the culture of the organization, allowing for long-term sustainability.

Another approach is to start by carefully considering the information needs of the business—who are all the relevant stakeholders, and what do they want to know? What are competitors leveraging this data for? How is achievement of the initiative measured?

It is also important to consider how the 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 easier to determine which tools and algorithms may be the best fit.

No one solution exists for all life sciences HCP engagement programs, and no customized solution will work in perpetuity. As the spotlight on these programs intensifies, and business processes grow more complex, life sciences companies should take an ongoing look at HCP engagement oversight through people, process, and technology. Continuous process improvement can help mitigate risk while also paying dividends to the company.

6. 2018 End-to-End Healthcare Professional (HCP)/Engagement Survey
9. Laura M. Kidd Cordova (Assistant Chief, Criminal Division, Fraud Section, US Department of Justice), August 16, 2016.
M&A

Mergers and acquisitions (M&A) remain a very strategic move in the life sciences industry. With M&A, compliance and ethics issues can have major impacts on everything from deal finances to future regulatory obligations to reputation. Yet those issues may not always be included in core due diligence. Below are some considerations as you evaluate transactions in the future:

- Deal finances
- Future regulatory obligations
- Reputation
- Regulatory compliance
- Manufacturing and distribution compliance
- Commercial compliance

Across the continuum of an acquisition or merger, appropriate compliance considerations can help ensure that inherent risks and liabilities are understood and considered in deal and integration structures.

Numerous deals have been abandoned in their later stages due to compliance and legal issues. Others were successfully completed, only to result in significant and unexpected liabilities for the acquiring entities.

**Some keys to achieving success throughout the M&A process**

It is critical to be aware of potential risk exposure and inherited liability related to compliance and to appropriately consider those factors in all phases of M&A. These factors include:

**Due diligence**
- Compliance representatives have a seat at the table.
- Core regulatory and compliance matters are contemplated in deal validity.
- Risk profile of the target’s business model is understood.

**Pre–day one planning**
- Compliance and regulatory representatives should be part of larger integration teams.
- Rapid risk assessment is conducted, as allowable.
- Position or operating model of the organization is determined to understand how to integrate compliance elements.
- Communication

**Post–day one integration**
- Continued risk assessment
- Policy and procedure integration
- Ongoing communication

Historically, compliance considerations have been an afterthought in M&A or have been managed as a low priority. However, given the level of risk presented by regulatory and compliance matters, compliance considerations should be carefully taken into account across the deal continuum.

Compliance and regulatory representatives should be closely involved in every M&A phase, from predeal due diligence through integration. Inherited liability, cultural and ethical differences, and policy and process disconnects can be extremely costly—in terms of regulatory obligations, reputation, financial outcomes, and the overall achievement of deal aims—and should thus be handled with the high priority they deserve.

**Let’s talk**

Chris Caruso
Partner
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
ccaruso@deloitte.com

Clarissa Crain
Senior manager
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
ccrain@deloitte.com
Using artificial intelligence in compliance management

To comply with regulatory requirements and manage risk, life sciences manufacturers implement controls to review and audit ongoing business activities. However, because it is not feasible to monitor and audit everything, compliance organizations have historically used a risk-based approach to set priorities and then monitor activities with the highest potential for compliance risk.

Now, thanks to advances in AI, life sciences manufacturers are exploring new ways to automate key elements of the risk identification, auditing, and monitoring process—and are capitalizing on opportunities to use data from monitoring in their strategic decision-making. These AI-driven improvements can help life sciences companies proactively identify anomalies, prioritize compliance risks accordingly, and manage investigations more effectively.

What is AI?
The standard definition of AI is “the capability of a machine to imitate intelligent human behavior.” Alternatively, instead of comparing it to human intelligence, AI can be viewed as a special type of computer programming that encompasses a number of distinct applications, including natural language processing, machine learning, neural networks, and many others (figure 1). These applications vary widely in sophistication, practical usage, and overall maturity.

Although AI takes many forms, the most common is rule-based AI: applying rules to data sets in order to achieve outcomes or results. For most rule-based AI applications, the programming is nonsequential; it does not follow a predetermined path to reach an outcome. Instead, rules “fire” when the data sets meet parameters that instantiate the logic contained in the rules to reach a final conclusion.

Even with its list of real-world commercial applications growing by the day, AI’s promise can still verge on overpromising. Compliance professionals should, thus, approach AI applications with a critical eye, but also with a willingness to meet those applications halfway. Like any form of programming, today’s AI is entirely dependent on the data it receives and the rules contained within the application. Currently, no AI system is capable of resolving issues as a self-contained system entirely on its own (autonomously acquiring data and providing a solution without human intervention). As such, collaborating with AI—rather than depending on it—is essential to unlocking the technology’s value.

Figure 1. Types and applications of AI

<table>
<thead>
<tr>
<th>Types of AI</th>
<th>Specific domains and applications of AI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Artificial super intelligence</td>
<td>Data extraction</td>
</tr>
<tr>
<td>Smarter than best human brains in every field</td>
<td>Content summarization</td>
</tr>
<tr>
<td>Artificial general intelligence</td>
<td></td>
</tr>
<tr>
<td>Solves, broad range of problems, like humans</td>
<td></td>
</tr>
<tr>
<td>Artificial narrow intelligence</td>
<td></td>
</tr>
<tr>
<td>Solves, narrow or specific problems</td>
<td></td>
</tr>
<tr>
<td>Progress as of today</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Machine learning</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Machine Learning is used to achieve AI (computer vision, NLP, BLG, etc.) It is also commonly talked about as a separate domain of AI focused on structured data analysis (e.g., anomaly detection, prediction).
Regulators expect real-time monitoring

Traditionally, manually driven compliance monitoring programs have had to rely on sampling (auditing subsets of transaction data extracted from source systems) in order to identify possible risks and anomalies. However, as AI applications are increasingly used to support compliance monitoring, the paradigm can shift from manually driven compliance monitoring and data sampling to near-real-time automated monitoring of all source data.

Near-real-time monitoring is a significant compliance management capability, whether implemented as a preventive measure or in response to regulator concerns. For example, recent corporate integrity agreements (CIAs) issued by the HHS’ OIG demonstrate that regulators expect compliance programs to have a comprehensive view of the activities they monitor. In addition, the DOJ’s focus on monitoring and compliance was reemphasized earlier this year when, on April 30, 2019, the DOJ updated its 2017 guidance related to evaluating the effectiveness of a compliance program. As the DOJ makes clear, compliance programs must be well designed, effective, and work in practice. Risk assessment and monitoring is essential to meeting those standards.

AI applications can help compliance teams conduct the thorough transaction reviews expected by the DOJ and OIG. For example, a well-designed monitoring program supported by AI applications can examine structured and unstructured data to provide compliance teams with a global view of interactions with HCPs; it can also provide insight into how independent charities and patient interactions are carried out in practice and then assess whether those actions align with internal and government policies. By
applying AI technologies to monitoring programs, companies can achieve a higher level of assurance at far lower cost than with a purely manual process while also lowering their risk profiles.

**Using knowledge-based and model-based approaches to identify risk**

Combining AI analysis with predictive analytics can enable modeling techniques to assess compliance risk on a prospective basis, helping users make timely and informed decisions to address identified anomalies. With insights from AI applications, monitoring risk data can become a far more useful tool for compliance officers and others. Machine learning can be used to comb through large data sets, not only to identify potential risk areas, but also to optimize use of resources and uncover performance trends in provider engagements that are difficult to identify through manual processes. For example, knowledge-based solutions can:

- Identify issues or patterns in appropriateness of physician specialty targeting (e.g., on- or off-label; NSAID prescription volume)
- Optimize the use of key opinion leaders: identifying the most appropriate health care provider to engage based on objective parameters, thereby maximizing the use of resources, identifying appropriate venues, and optimizing budgets.

A well-developed risk management rule base—coupled with a machine-learning architecture—can detect anomalies across the full range of monitored activities. Also, it can apply its insights to identify patterns of action or behavior for compliance teams to consider (both for real-time intervention and to further refine the rule base itself). With these advances, compliance programs can move beyond sampling and spot checks to analyze the full universe of activities they monitor.

**Enhancing pharmacovigilance with AI**

Case processing is the central activity for pharmacovigilance (PV) programs. With the advent of biologics and the availability of treatments for more complex disease states, the operational and compliance challenges related to pharmacovigilance (PV) have grown in parallel (figure 3).

Traditionally, any monitoring beyond self-reporting of adverse events (AEs) has required manual review of emails, phone calls, and structured data sets. Often, the massive amounts of quality and
outcomes data needed for PV activities reduces the overall capacity for informed, human clinical decision-making. PV programs can thus become bogged down by processes and struggle to meet a growing array of regulatory requirements.

A well-designed AI platform aggregates disparate data sources and applies advanced machine learning capabilities to allow for more targeted human intervention. The crucial design lesson is to view AI not just in terms of technologies, but also in terms of its impact on processes and on the people needed to detect, assess, understand, and help prevent safety-related issues. Figure 4 shows how machine learning can be applied to improve and streamline PV case processing.

AI’s power to aggregate and standardize diverse data streams is at the heart of its value to life sciences organizations. Making structured data out of multiple unstructured inputs can have significant uses beyond case processing. Once the required data management structure is put in place, the intelligent learning mechanisms behind cognitive case processing can also generate highly salient information for safety surveillance, benefit and risk analysis, compliance management, and even commercial insights.
Putting it all together
Although automation and AI can save time and money, implementation can be a challenge. Some keys to an effective outcome include:

- Start with a limited proof of concept (POC) and then evolve the application by gradually increasing its functionality and scope
- Define functionality, compliance rules, and human interaction requirements before selecting technologies or creating the overall design

The following three-phase approach has been effective when deploying automation and AI (figure 5).

Limiting the initial scope to a proof of concept enables the implementation team to test the rule sets, refine the knowledge base, and then apply a logical approach to expanding the functionality. Once the proof of concept is developed and the application has met its design goals and objectives, the team can review the existing and planned architecture in order to evolve the POC, incorporating additional functionality in accordance with the plans developed in phases one and two.

The present and future of AI in compliance management
As regulatory pressures mount and data grows in scope and volume, human intelligence alone cannot keep up with the vast amount of information that compliance programs are expected to monitor. AI capabilities can enhance monitoring programs by:

- Increasing the amount of data that can be reviewed
- Increasing the frequency that audit routines can be implemented
- Identifying anomalies
- Prioritizing compliance risk
- Managing possible resultant investigations

Figure 5. Steps to consider when deploying automation and AI

1. **Build an automation strategy & execute an automation assessment**
   - Build an automation strategy that defines the vision, strategic objectives, and goals for the program
   - Analyze the existing inventory of processes and tests to identify automation/modernization candidates using defined automation Risk and Fit criteria
   - Document quantifiable benefits (quality, FTE time/cost savings, etc.) that can be achieved and execute a cost benefit analysis
   - Prioritize a list of targeted areas to explore modernization or automation opportunities

2. **Develop priority use-cases in workshop lab**
   - Facilitated environment that allows decision makers to explore the benefits of modernization and technology
   - Develop a clear modernization plan with robust and practical ideas for applying RPA & CI to enable increased efficiency and effectiveness
   - Potential use-cases mapped to appropriate technology or process optimization
   - A roadmap for adoption of RPA & CI

3. **Execute a proof of concept**
   - Demonstration of the concept of RPA & CI, where a prototype robot (“bot”) is created for a pre-selected process or activity
   - Illustrates the benefits that can be derived through bot implementation and provides critical inputs for broader implementation of RPA & CI in the future
   - Model process for enterprise wide adoption with list of potential organizational roadblocks and hurdles
As knowledge bases become more robust with compliance rules—and learning algorithms become more advanced—we expect AI to become more integrated into the compliance monitoring regimen. Life sciences manufacturers should start small with a proof of concept application focused on one area of compliance risk, then eventually expand to additional risk areas once the technology has proven its worth.
Additional regulations and trends

A number of external and internal forces and trends are placing additional pressures on life sciences companies’ compliance programs. These include renewed public interest in how life sciences companies are operating, the opioid crisis, the cost of drugs and therapies, and the lobbying efforts and involvement of the industry in politics— all of which continue to affect how the government conducts its oversight. Regulators are requiring compliance programs to operate at a higher level. At the same time, new pricing and privacy provisions continue to become law as drugs take center stage in the political debate around health reform.

Both the life sciences marketplace and its regulatory framework are changing, and compliance professionals need to change their own business practices accordingly. In the year ahead, the challenge for life sciences companies’ compliance programs will be to create and maintain a comprehensive approach to risk that is nimble enough to respond to a more complex, higher-stakes regulatory environment.

**New pressures from the government**

Recent guidance from the DOJ illustrates how regulators are stepping up their oversight role and demanding more from the companies they monitor. The DOJ’s updated guidance on how prosecutors should evaluate compliance programs explicitly states that a continually evolving and proactive approach to compliance is no longer optional for life sciences companies.

Although many of the concepts in the guidance have been discussed for many years by the DOJ, settlements and CIAs still occur on a regular basis. As the new guidance makes clear, “paper compliance” is not enough. Going forward, prosecutors will take the demonstrated effectiveness of a compliance program very seriously when determining how to pursue enforcement actions.

If a culture of prevention (as well as detection and correction) is front of mind for regulatory enforcers, then it should be the same for compliance programs. Also, aside from how the law is being interpreted and enforced by prosecutors, the scope of risk itself is changing. Digital technologies that are becoming common parts of life sciences products and marketing are often outside the purview of laws written decades ago. A culture of prevention should, therefore, look beyond what prosecutors are saying and carefully examine the practical implications of market shifts such as digitization.

While sweeping reforms such as Medicare for All remain possible over a two-to-three-year time horizon, more immediate legislation could have meaningful impacts in 2020. Drug-pricing legislation in the US House and Senate each call for new reporting requirements and pricing references that pose additional risks for life sciences firms. Companies might be required to publicly post WAC price increases or be given new mandates to issue rebates for price increases that outpace inflation. In all instances, the potential penalties are severe, with the Senate proposing the removal of sanctioned entities from federal programs and the House proposing steep excise taxes for companies that do not negotiate prices with the federal government.

**Industry changes**

At the same time that the regulatory landscape is shifting, changes in the industry itself present new considerations for life sciences compliance professionals. Nontraditional mechanisms of action and products that straddle traditional industry categories such as pharmaceuticals, biologics, or medical devices have new risk profiles both for premarket approval and during postmarket vigilance. In some cases, the law is ambiguous or silent on which regulatory body is ultimately responsible for certain aspects of product safety or whether a particular therapy should be categorized under one pricing mechanism or another.

Life sciences companies themselves are also changing. Recent M&A indicates a growing interest among life sciences companies to enter new market spaces, such as diagnostics and cellular therapy, or to work with companies that have historically operated in other sectors. Despite due diligence efforts, new partners might be unaware of existing risks within acquired assets; also, entering a new industry can present a fresh (and often unknown) set of compliance concerns moving forward.

Even with successful due diligence, any merger or acquisition will require the integration of both legacy compliance systems and company culture in a heightened enforcement environment.
Putting it together: Current and emerging risk areas

The confluence of renewed enforcement and a fast-changing industry requires enhanced vigilance on the part of life sciences companies’ compliance programs. Compliance professionals are typically quite familiar with the Office of the Inspector General’s policies and procedures and the PhRMA Code on Ethics with Health Care Professionals. However, shifting industry practices and regulations mean that a “check-the-box” compliance approach that follows the rules as they are written will likely not be sufficient to address new risk areas.

To be efficient and effective today, compliance professionals should become experts in matters beyond the scope of the past. Every compliance team in the life sciences industry should examine the full scope of its unique product portfolio so it can anticipate and respond to specific compliance concerns that might not be common across the industry. Also, where life sciences companies are working with business partners in an unrelated field, compliance teams should coordinate closely with their counterparts and identify what they themselves need to know about the risks a partner might bring.

The growth of interoperable devices and remote patient monitoring provide examples of how current and emerging risk areas combine, with new concerns about data security emerging as well. Companies that have not dealt with protected health information in the past might not be familiar with the extensive oversight and controls needed to mitigate risk. In addition, recent incidents where hospital systems were infected with ransomware point to a future where any entity that houses or transfers vital patient data is at risk of being targeted.

The federal government has taken notice of these challenges. For example, recognizing that the HIPAA does not cover devices such as smart watches (which have traditionally not been categorized as medical in nature), 2020 may see a new legislative push to update the HIPAA privacy provisions for the modern age.

Another example is patient support services (PSS), which received significant attention from regulators in 2019. A number of life sciences companies have been issued subpoenas related to a variety of program elements (e.g., field nurse programs, copay programs), entered into settlements of civil and criminal PSS-related matters, CIAs, and answered congressional inquiries.
While risk management has not been a traditional priority in patient services, the dependence on third parties (such as HUBs and distributors) to operate high-touch, high-cost, specialized programs brings a host of compliance considerations, ranging from Anti-Kickback Statute and False Claims Act exposures to drug safety and pharmacovigilance. PSS programs for products that cross multiple therapeutic categories add yet another layer of complexity for compliance professionals.

Third-party vendors present other more basic logistical concerns as well. The universe of third-party vendors that life sciences companies rely on to carry out patient interactions uses a variety of different data standards, creating an added challenge for software used to monitor data, such as financial transactions that are otherwise relatively straightforward.

Compliance front and center
In today’s complex market and regulatory environment, compliance programs must be well designed, effective, and practical. Risk assessment that combines both insider and outsider perspectives is essential to meeting those standards. Also, given the combination of an enhanced regulatory regime and a fast-changing industry that involves more players than ever, a centralized and automated compliance approach supported by advanced analytics that can provide a global view is now indispensable.

While 2020 will bring greater scrutiny to an already complex industry, emerging technologies such as robotics and cognitive automation are constantly evolving to help tackle the challenges. These technologies hold great promise to help compliance professionals do more with less; however, they cannot function effectively without trained staff, clear processes and protocols, and a governance structure that incorporates compliance concerns into all business matters.

Ultimately, with so many complex issues in play, life sciences companies’ compliance teams will need a seat at the table during strategic conversations on product development and M&A and when trying to make sense of a constantly changing regulatory environment. Proactive compliance is no longer optional in life sciences; as such, it is no longer viable for the compliance function to stand apart from other aspects of the business.

Let’s talk

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

Clarissa Crain
Senior manager
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
ccrain@deloitte.com

Ashley Riley
Senior manager
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
ashriley@deloitte.com
Staying ahead

The regulatory landscape is constantly shifting. Some changes are big enough to grab headlines. Others are nearly invisible but can have a big impact. For the latest regulatory updates and insights, please visit www.Deloitte.com/us/LifeSciencesRegulatoryOutlook.

Leadership

Alok Sinha
Regulatory & Operations Risk leader
Principal | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
asinha@deloitte.com

Dan Ressler
Advisory Life Sciences industry leader
Principal | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
dressler@deloitte.com

Paul Silver
Life Sciences Regulatory & Compliance leader
Principal | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
psilver@deloitte.com
This article contains general information only and Deloitte is not, by means of this article, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This article 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 adviser. Deloitte shall not be responsible for any loss sustained by any person who relies on this article.

About Deloitte
As used in this document, “Deloitte” means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2019 Deloitte Development LLC. All rights reserved.