MEETING THE CHALLENGE OF IT COMPLIANCE IN LIFE SCIENCES

BioSource Advisors

A COMPLEX MANAGEMENT CHALLENGE

Life science organizations in the U.S. operate in one of the most rigorously regulated industries in the world. From venture-funded biotechnology and genomics startups to commercial-stage pharmaceutical and diagnostics companies, all must comply with a host of regulations designed to protect patient safety, safeguard the privacy of personal health information, and provide greater transparency. Moreover, the compliance landscape is not static, with ongoing rule changes that challenge organizations to continually evaluate and update their processes and controls to avoid falling out of compliance. This reality has placed ever-more responsibility on the shoulders of corporate compliance officers.

At the same time, the role of information technology within the life sciences industry has continued to expand. IT systems, applications and networks are inextricably woven into the fabric of life science organizations of all stripes—from researchers to pharmaceutical manufacturers to medical device makers. All rely on IT systems and data to facilitate everything from clinical trials and R&D to product commercialization and customer support. This compounds the complexity of the compliance challenge.

THE COST OF NONCOMPLIANCE

The financial impact of noncompliance can be crippling. In 2021, data breach costs rose from $3.86 million to $4.24 million, representing the highest average total cost. In addition to causing tremendous damage to a company's reputation and brand, a breach of protected health information (PHI) or other serious compliance failure could expose the organization to significant fines if regulators deem the company's safeguards were inadequate.

Data breaches are not the only risk; there are many potential compliance pitfalls for life science organizations. For example, in 2019 the state of Nevada's Department of Health and Human Services levied more than $17 million in fines on 21 diabetes drug manufacturers for non-compliance with the state's price transparency law. Passed in 2017, the law requires diabetes drug manufacturers to submit annual reports on its costs, profits, and other information related to product pricing.

ORGANIZATIONAL CHALLENGES

Despite the significant risks posed by non-compliance, staffing in compliance and security departments is limited in many life science organizations—especially in early-stage companies. Compliance officers often find themselves overworked, as they struggle to manage an increasingly complex matrix of rules and regulations, many of which involve the use of technology.

The heightened role of technology in business operations also frequently causes a mismatch between the skill set within the compliance department and the technical requirements that must be addressed. Compliance professionals may not be aware of potential vulnerabilities within the IT infrastructure that could expose sensitive data—including protected health information (PHI) and valuable intellectual property (IP)—to cyber theft. The rise of distributed computing models and cloud computing compounds the potential risk, as critical data and applications are increasingly housed outside the enterprise data center. Even more concerning is the fact that in-house personnel may "not know what they don't know," making it difficult for them to assess their compliance risk.

THE INTERSECTION OF COMPLIANCE AND IT

Life science companies must by law comply with a host of federal and state regulations that involve technology and data protection. These include the following:

FDA Title 21, CFR Part 11

The U.S. Food and Drug Administration's (FDA) Code of Federal Regulations (CFR) Title 21, Part 11 is designed to ensure the reliability and accuracy of electronic records and electronic signatures. Part 11, as it is commonly called, requires that FDA-regulated entities implement effective controls for systems that process data. This includes audits, audit trails, system validation and documentation, record retention, and other controls to ensure the integrity of electronic records subject to FDA regulation.

Data security is a key focus of Part 11. Compliance requires effective controls relating to system access, including defined roles and permissions, strong passwords and defined lockout mechanisms. This ensures that only authorized users can access the information —including both company employees and external third parties, such as Clinical Research Organizations (CROs) and suppliers of biospecimens for research.

The proper use of eSignatures is also a focus, ensuring that identities of signing individuals can be verified with confidence. This is normally accomplished using third-party software or software-as-a-service (SaaS) offerings.

Traceability is another important aspect of Part 11. Companies must have clear audit trails to show which user performed what specific actions to records, and at what time, with version control information. This must be readily accessible to FDA auditors performing periodic inspections.

Health Insurance Portability and Accountability Act (HIPAA)

The federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) sets forth requirements for protecting the confidentiality of protected health information (PHI). This includes information about an individual's health status, provision of healthcare, or payment for care. In fact, HIPAA defines no fewer than 18 identifiers that must be handled with care—from names, social security numbers and email addresses to geographic locations and personal biometric identifiers. Ensuring systems and processes support compliance with strong data protection is a critical step for HIPAA compliance.

One area of HIPAA that is often overlooked is the requirement that business associates (BAs) of regulated entities comply with HIPAA requirements concerning protection of PHI. This applies to any third party who accesses this data for the purposes of performing their work. Organizations should take care to craft BA agreements that clearly describe the permitted and required uses of PHI by the business associate and define appropriate safeguards.

Health Information Technology for Economic and Clinical Health Act (HITECH)

The expanding role of data—including personal, non-public health data—in the healthcare and life sciences sector led to the enactment in 2009 of the Health Information Technology for Economic and Clinical Health (HITECH) Act which regulates the use of digital media and systems for handling non-public health information.

The HITECH Act gave additional strength to HIPAA enforcement, including significant penalties for willful neglect of PHI safeguards. The Act gives individuals the right to obtain their PHI in electronic format and requires that patients be notified of any unsecured data breach. For a breach impacting 500 or more patients, the U.S. Department of Health and Human Services (HHS must also be notified, triggering public dissemination of the name of the non-compliant entity. This exposure can damage a life science organization's brand and reputation, and diminish its prospects in the eyes of potential investors.

HIPAA and HITECH non-compliance can be extremely costly. In the first half of 2021, HIPAA fines were levied against 100 organizations and topped $130 million. The risk of fines is not limited to large organizations and health systems. In mid-2021, the OCR fined Peachstate Health Management, LLC, doing business as AEON Clinical Laboratories, a diagnostic laboratory in Georgia, $25,000 for HIPAA Security Rule violations.

Sarbanes-Oxley Act (SOX)

Publicly traded organizations must also comply with the Sarbanes-Oxley Act of 2002 (SOX). Key technology-related requirements include the need to establish and enforce policies governing how accounting systems and other systems handling financial data are developed, modified and maintained. In addition, safeguards must be in place to prevent data tampering and protocols for responding to data breaches must be developed and followed. Access to sensitive personal and financial data must be monitored and recorded.

Even though SOX compliance is not required for privately owned companies, it represents a set of best practices for managing risk. For venture-funded life science organizations, adopting SOX compliance early in their progression can help ease the transition if and when they go public or are acquired by a publicly traded company

Other relevant regulations

Organizations that produce life science products should also comply with Good Manufacturing Practice (GMP) standards. Derived from FDA regulations, these standards help ensure that products are consistently produced and controlled according to quality standards. Technology systems play a central role in assuring and documenting quality processes throughout the production lifecycle.

In addition to federal rules, life science organizations may need to comply with state regulations or guidelines. These often include specific reporting requirements that differ from one state to another. While compliance officers will be familiar with rules regarding their financial controls in the states in which they operate, they may not be aware of what is required to ensure their IT platforms support compliance. For firms operating in multiple states, keeping track of these issues can be extremely complicated.

With continually evolving regulations and cyber threats increasing in both frequency and sophistication, maintaining compliance is a complex and time-consuming task that never ends.

As noted previously, life science organizations may not have the in-house resources to effectively address the technical aspects of complying with these regulations and best practices. Moreover, compliance is not a “one and done” proposition; with continually evolving regulations and cyber threats increasing in both frequency and sophistication, maintaining compliance is a complex and time-consuming task that never ends.

COLLABORATION SOFTWARE AND COMPLIANCE

Another factor affecting compliance risk is the ubiquitous adoption of collaboration software, including cloud-based collaboration platforms. These include productivity products like Google Docs, conferencing solutions like Zoom and Skype, and file sharing tools like DropBox. By enabling knowledge workers to easily exchange information and collaborate with colleagues and external partners anytime, anywhere in the world, these tools offer attractive efficiencies. However, they can pose significant vulnerabilities for companies with regard to protecting sensitive data and complying with rules governing document retention. Critically, the firm may not even be aware that employees are using these popular platforms or, if they are authorized, whether employees are using them compliantly.

A recent industry survey found that more than 70% of IT and cybersecurity professionals expressed concern about safeguarding and archiving data from these platforms. Ensuring the organization has clear policies governing the use of such platforms, informed by a robust understanding of relevant regulations and industry best practices, is crucial. These policies and their enforcement mechanisms must be regularly reviewed and updated as needed to ensure continued compliance.

DUE DILIGENCE REQUESTS

For companies actively pursuing investor support, merger and acquisition opportunities, or strategic partnerships, a common challenge is a request for due diligence questionnaires (DDQs). Companies must be able to substantiate in detail the measures they have in place to safeguard data. Yet many compliance departments may not have the time and/or technical expertise to complete these DDQs satisfactorily, or their compliance and cybersecurity measures may not be up to the requisite standard. Both circumstances could threaten a deal essential for the company's research and/or commercialization.

A COMPREHENSIVE COMPLIANCE STRATEGY

Because technology is so central to the operation of life science organizations, a comprehensive strategy for IT compliance must encompass three key elements—the Three Pillars of IT Compliance:

1. DEFINED POLICIES

The company should have clear, written policies regarding aspects of technology that impact or contribute to compliance. To ensure people throughout the organization take them seriously, these policies must have senior leadership buy-in and active enforcement.

2. EFFECTIVE SYSTEMS

The company must have systems in place to ensure compliance is maintained. This includes robust perimeter security and monitoring systems to guard against unauthorized access to platforms and data.

3. ATTESTATION

The company must have up-to-date reporting to satisfy compliance audit and exam requirements, and to keep compliance officers and senior leaders informed of the state of their compliance posture.

Weakness in any one of these three areas could cause an organization to fall out of compliance—or, worse yet, expose their firm and its clients to risk, including the very serious consequences of cybercrime.

A comprehensive strategy for IT compliance must encompass three key elements: defined policies, effective systems and attestation.

KEY SUCCESS FACTORS

To satisfy the Three Pillars, organizations must ensure compliance across their entire technology infrastructure, including the following key factors:

Vulnerability Assessment

A comprehensive assessment of systems and processes is needed to reveal compliance gaps and/or potential vulnerabilities. This analysis provides valuable insight and actionable steps to address IT issues that could present compliance risk. Ongoing monitoring and assessment of potential risks is needed to keep abreast of changes that impact IT platforms.

Compliance Policy Creation

This step involves crafting compliance policies to mitigate risks identified in the vulnerability assessment, tailored to your business processes and IT environment. Authoring effective policies requires a deep understanding of both the IT infrastructure and the rules, regulations and best practices relevant to your organization—whether it is a publicly traded company or a venture-funded startup. These policies must be reviewed and revised to keep pace with changing compliance requirements and evolving technologies.

Access Management

Ensuring only authorized parties are able to access sensitive data is a critical step in compliance. Identifying potential intrusion risks early and closing the door on these vulnerabilities is a complex task, given the ever-changing cyber threats that target the life sciences sector.

Intrusion Detection and Response

Continuous threat intelligence ensures that you are always equipped to detect threats as they emerge. The most proactive intrusion detection platforms are fully integrated with robust threat intelligence that provides security analysts with critical context. Ideally, threat intelligence will come from a variety of sources, including the open source community. In the event of a breach, having systems and procedures in place to limit and mitigate the damage, and capture forensic data is essential.

Cloud Management

While public cloud services are growing in popularity due to their convenience, they may not provide the level of security demanded to ensure compliance with data protection and documentation regulations. A purpose-built private cloud solution, developed to meet the specialized needs of financial organizations, can provide compliance assurance while offering all the advantages of cloud computing platforms.

Backup & Disaster Recovery

A robust backup and disaster recovery solution is critical for preventing business interruption and loss of critical data, which could trigger a compliance violation. Off-the-shelf, onsite backup solutions do not provide the level of performance required to meet the needs of financial organizations. Having the ability to perform frequent, granular backups of all systems and data, with secure data encryption at all points and rapid recovery, are essential success factors.

WHAT TO LOOK FOR IN A MANAGED SERVICE PROVIDER (MSP)

To fulfill the Three Pillars of IT Compliance, it is important to work with an MSP that combines several key characteristics:

Compliance Expertise

The MSP should be thoroughly familiar with regulations, rules and best practices applicable to the life sciences industry, including both federal and state regulations for all jurisdictions in which your firm operates. They should be able to point to a track record of success serving firms in your particular industry sub-segment.

Breadth of Services

The MSP must be able to provide a comprehensive solution that encompasses all of the strategic pillars described earlier. This facilitates a holistic approach, eliminating gaps in IT management that could cause compliance lapses (and the "finger pointing" that can result) while ensuring you have a single, capable partner taking accountability for helping ensure the compliance of your entire IT infrastructure.

Scale

Ramping up internal IT departments is costly and time-consuming. Small, “boutique” MSPs face the same challenge and often cannot scale to meet expanding needs as your firm grows—especially if that growth involves expanding operations into other jurisdictions. Working with an MSP that has a critical mass of professional resources and national reach provides the scalability needed to handle whatever the future brings.

Superlative Service

Your clients expect a high level of service and that’s what you should expect from your MSP. They should demonstrate the ability and willingness to provide rapid, effective service and support to your firm’s users—including special support for VIPs, such as home visits if required