MAYNARDNEXSEN

Cybersecurity and Data Management for Life Sciences Companies: Key Considerations and Issues for Leadership

Related Professionals

Joseph A. Dickinson, CHPC
919.678.7592
JDickinson@maynardnexsen.com

Matthew B. Roberts
803.253.8286
mroberts@maynardnexsen.com

Practices

Intellectual Property Law

Life Sciences

Article
10.12.2022

Cybersecurity is an issue that crosses all industries and businesses. That said, companies in the life sciences space, in particular, are seeking guidance given the fast pace of change in the legal and regulatory requirements they face. The topics of data privacy, security, and information governance are keeping life sciences executives up at night, wondering if they are doing enough, or even doing the right things. The issue is even more impactful in the context of life sciences because these organizations are dealing with such critical and sensitive data including health information protected by HIPAA, trade secrets, and other important intellectual property as well as protected data from other third parties. Management of that data is challenging because of the risks associated with coordinating information from a variety of sources. In addition, the transformation to the use of digital technology in the life sciences space has increased cybersecurity risks. In this brief article, we address several topics that leaders in the life sciences space have been asking about when faced with managing data.

What are some of the key misconceptions around data privacy and security that seem prevalent in the life sciences industry?

Don't Confuse Data Security with Confidentiality

Some leaders confuse privacy and security with confidentiality. They think as long as they keep information and data confidential, they've done what they need to do. They also believe that once patient information is acquired it can be used for any purpose as long as they keep it secure. There is a frequent failure to recognize that having access to the information for a specific purpose (which is often the case

with life sciences) doesn't mean that it can be used for other purposes, including further disclosure internally or to third parties. Not appreciating that there are many detailed and specific restrictions on the ability to access, use, and share patient information is a key misconception. In most cases, there are legal and regulatory obligations to protect that information. As an example, when information is made available for clinical research, there is a belief that secondary and collateral uses beyond the research are appropriate as well, and in many cases that is not true.

Standards Do Apply

Life sciences companies often are not aware of or don't fully understand the standards for protecting data that apply. Many of these standards are inherited, by contract terms or otherwise, from the companies and health care systems that serve as the source of the information. These standards and obligations may vary but they are no less important and in many cases, are broadly applicable. In particular, where research or pharma companies are collecting or acquiring information specific to patients, including for the purposes of clinical trials, that data is typically subject to multiple obligations for keeping it private and secure. Those obligations often go beyond the initial purpose that is relied on for accessing the research.

How are life sciences companies, including clinical research organizations, impacted by privacy and cybersecurity requirements?

Origin of Data

Life sciences companies often have access to information from a number of sources. When we assist with risk assessments and audits, we often find gaps in the management of the information and particularly the management of the source of the information as a contributing factor in the restrictions that may apply. Many organizations are not keeping the origination of that information as part of the "metadata" that is monitored.

Contractual Obligations

It is not always only the patient information that could be covered by HIPAA. Often it is not the regulatory requirements that we see as the source of the problem - it's the contractual terms and the boilerplate language that cause problems. Many companies that are required to comply with HIPAA or GDPR, or any number of other privacy/security regulations, have language built into their boilerplate agreements that pass on to other life sciences companies these obligations through contractual commitment. When these contract terms are overlooked or ignored, it creates a failure to comply with those obligations which can have a significant impact on liability and business relationships.

Many companies forget about the "white noise" that is included in those contracts and the boilerplate language – particularly in areas where they are shifting the risk of who is responsible for the data that is being shared or stored or used.

Paper vs. Reality

Another problem often seen during risk assessments and compliance audits is that the paper doesn't match the reality. Organizations often take a checklist approach – marking off boxes as they go. Do they have the right policies, website terms of use, and the right contract terms? Once they check the box acknowledging that they have addressed those issues on paper, they believe they've addressed the compliance issue. But technology changes, and business relationships change – your cloud service provider for data services today may not be who you are using next week, so the representations you've made in your "paper" very frequently get outdated. We find risk for life sciences organizations because there is a disconnect between what they say they are doing and what they are actually doing with data. Companies have numerous privacy and security controls in place, but they are often not well documented, updated, or continuously monitored and controlled. There needs to be a living/breathing program of data management, not just a checklist.

It is Not an IT Problem

Senior leadership should be actively involved in deciding, implementing, managing, and auditing the privacy and cybersecurity programs at any life sciences organization. Most legal/regulatory requirements contemplate that senior leadership and boards of directors are actively involved in protecting the privacy and security of data. There is a tendency for leadership to want to hand these responsibilities off to an IT department or specialist. The day-to-day operational aspects are one component. However, the strategy and management components are not just an IT issue or a compliance issue. They are more about asset and risk management and the impact on the top-line and bottom-line on the financial statements – issues that senior management is primarily responsible for addressing.

False Sense of Security

We are all aware of data breaches in virtually every industry and commercial space, but at times there is a mentality that "this couldn't happen to us." Management may believe they are too small, or their data is not as valuable, or they are safe because they have policies, firewalls, and state-of-the-art technology that protects them. There is a false sense of security when company leaders don't see their competitors or others within their industry on the front page news with either a breach or regulatory enforcement action due to a data breach. However, there remains a tremendous risk – both organizationally and financially. The majority of the problems don't stem from regulatory enforcement actions but more from the "private enforcement" actions. Businesses lose revenue and customers because they are not able to provide adequate privacy and security. The value of a business deal can go up or down depending on the privacy and security controls of the seller or company seeking investment dollars. Because of the nature of life sciences companies, they are more exposed to this risk than companies in other industries.

One example is a recent case where a company was being acquired and expecting to receive $XXM at closing. A problem arose because the acquirer was an international company with a significant presence in healthcare with GDPR, HIPAA, and other regulatory obligations for protecting the privacy and security of data. The target company had never addressed any privacy and security controls making the full extent of the potential exposure

virtually impossible to quantify. As a result, the expected payment at closing became an earn-out. It is the "private enforcement" component that you rarely read about on the front page of the news that is a primary driver of why organizations need to pay attention to these issues.

Don't Be the Victim Twice

We often talk about trying to help our clients not be a victim twice – first by being hacked or when they have an incident, and a second time when there is a regulatory enforcement action, private litigation, or adverse contractual or business relationship consequence. For multiple reasons, it is usually more costly to deal with a data incident after it occurs as compared to managing the processes and planning on the front end. In addition, when thinking of regulatory enforcement actions, penalties or settlement fees, and the other consequences, including revenue loss and business reputation damage, remember that the Monday morning quarterbacks will look at what you do – your behavior before and after something goes wrong. They will look at your incident response plan, but when assessing potential liability and the level of culpability, they almost always look at what you did on the front end – how proactive you were in your prevention and protection efforts. They want to know that you've been reasonable and that you have a culture that prioritizes the privacy and security of information. So they look at what you did before the breach/incident when they are assessing how reasonable your controls were.

We have stressed the importance of preparing and being ready to respond. We have also looked at doing what is necessary on the front end. What do you say to someone who has thrown their hands up and said, "I don't know where to start."

Do Something

The worst thing you can do is throw your hands up and say there are too many laws, it's too complex, too resource intense, too expensive – and do nothing. When you think about all the things that can happen, regulators and others wanting to hold organizations responsible for their handling of information expect "reasonableness," at the very least, and doing nothing can never be defended as reasonable. So whatever it is you decide to do – do something.

Start by assessing what information you have about your data. Where is it? How is it processed? What type of information is it? In the legal and regulatory community, small companies do not necessarily get a break on the front end. Whether you are a small startup or a large business with thousands of employees, your obligations on the front end to understand how you collect and what you do with data are much the same. You have to assess what you do with the data and do what you can to protect it. All organizations should create a data inventory and a data map showing the flow of data. They should have a full understanding of what they are doing with data.

Have a Response Plan

The second thing to do is to come up with reasonable policies, procedures, and incident response plans for handling problems as they arise.

Monitor Your Vendors

A third item to consider that is key for health care and life sciences companies is to look at their vendors and ensure they are taking the proper steps to protect data. In the health care space, companies monitor their business associates – it's a requirement with HIPAA. Regulators want to know that you are actively managing your vendors and holding them responsible when it comes to data privacy and security.

Managing and protecting data is an important priority for life sciences companies. Nexsen Pruet works with life sciences companies to help protect their data and develop strategies to minimize and manage their cybersecurity and data management risks. We also assist life sciences companies after a breach or cyberattack has occurred to correct the problem and ensure it will not happen again.