CONNER
STRONG &
BUCKELEW

Originally published on the MassBio blog

Insurance Policy Pitfalls: Patient Data Security

BY DAN BRETTLER, LIFE SCIENCE PRACTICE LEADER, CONNER STRONG & BUCKELEW

Patient data continues to be highly sought-after by hackers, evidenced by the fact that 90% of all healthcare organizations suffered at least one data breach in 2014-2015.

In fact, hackers are now looking to exploit vulnerabilities in all corners of the industry. Life science firms have always been considered high-value targets because of the IP stored in their systems, but today hackers are also looking to these companies as a source of valuable patient data.

Because many life science firms believe they've washed their hands of sensitive patient data, for example by outsourcing clinical trial operations, they may overlook subtle exposures and not consider the value of insurance coverage. Yet the financial and reputational impacts of a patient data breach can be significant.

Life science executives turn to three common refrains when asked about patient data protections. Let's examine why these don't always stand the broker test.

#1: WE DON'T COLLECT PATIENT DATA.

Even if you're not in the business of formally collecting patient data, there may still be patient-identifiable data stored in your systems.

For example, adverse event reports are required to include an identifiable patient, an identifiable person reporting the event, a suspect drug or product, and an adverse experience or outcome suspected to be related to the product. This enables the FDA to properly investigate a reported incident. But it also means this information is likely filed away in your systems.

Companies that offer reimbursement counseling services may also be storing patient data. Patients are often required to sign authorizations that allow physicians or pharmacists to disclose their information to drug companies as part of the reimbursement process.

> “Hackers are now looking to exploit vulnerabilities in all corners of the industry.”

#2: MY INSURANCE COMPANY HAS ALREADY ADVISED HOW MUCH COVERAGE WE NEED.

When applying for cyber insurance the first time around, you probably completed your application based on known vulnerabilities and needs. Your insurance company then underwrote a policy based on your application. But if at any point you overlooked sensitive data buried within your systems during the insurance application process, you could run into to a disclosure issue with your carrier down the line.

Your policy might currently provide basic protections in the event of an employee data breach, in which case you may be on the hook for credit monitoring but not much more. But the conversation changes if any patient data resides in your systems. Those vulnerabilities will come with more severe monetary damages in the event of a breach, not to mention the loss in brand equity.

It's important to understand what sensitive information your company may be hosting – intentionally or inadvertently – and to discuss appropriate coverages with your broker.

#3: I'D RATHER BET ON MY IT TEAM THAN BET ON THE BAD GUYS.

Some companies determine the most effective way to spend on cyber defenses is to funnel funds into IT measures rather than insurance coverages.

But the evidence paints a grim picture for cyber defenders. The annual Ponemon Institute study of healthcare data breaches found that more healthcare organizations are experiencing data breaches now than six years ago. Despite advancements in defense strategies and technologies, hackers continue to outpace the industry.

As companies continue to fill their management teams, corporate boards and audit committees with cyber experts, there will be a more urgent need to secure comprehensive cyber insurance coverages, in addition to getting the right tools in place. A skilled insurance broker can help you determine your vulnerabilities and the most effective ways to cover them.

Originally published on the MassBio blog

CONNER
STRONG &
BUCKELEW