

As Security Breaches and Fines Grow, More HIPAA Entities Consider the Protection of ‘Cyber Insurance’

Reprinted from REPORT ON PATIENT PRIVACY, the industry's most practical source of news on HIPAA patient privacy provisions. Available online at: <http://www.aishealth.com/Products/HIPAA.html>

Hemophilia of Georgia has never had a privacy or security breach. Information is encrypted, security systems are tight, and privacy policies are strong, enforced and followed.

So why did the health care organization, which provides medication and support services to patients statewide, recently purchase a “privacy and network liability policy”?

Karen Geney, who pulls quadruple duty as the privacy officer, security officer, compliance officer and vice president of human resources, cites two reasons: fear of something going wrong, and peace of mind that costs would be covered if it does.

“We are very careful and always have been,” she says. “We have pretty much been overdoing everything” in terms of privacy and security precautions, especially because in the past there was such a stigma attached to hemophilia due to the number of people who contracted AIDS from blood products. “I hope we don’t need to use the policy,” Geney says.

While policies vary, some general categories of coverage are:

- Privacy liability,
- Network security liability,
- An identity theft response fund,
- Internet media liability, and
- Cyber extortion.

The first three categories are mandatory in a policy, as offered by some insurers.

Experts began recommending privacy and security liability coverage, sometimes referred to as “cyber insurance,” due to the increased penalty provisions in the HITECH Act and to cover losses that might arise due to misdeeds by entities new to HIPAA, such as subcontractors and agents.

In addition, a high-profile case that illustrated the potential value of such insurance has gotten the attention of many in the HIPAA world. The University of Utah has been unable to cover the expenses associated with a breach it had because the document storage company responsible for the loss didn’t have privacy insurance coverage, and its general insurer refused to pay for the costs.

In Geney’s case, the policy makes sense, says David Navetta, a principal with the Information Law Group, based in Denver. “For small businesses, a data security breach can literally mean going out of business,” he says. “That is why insurance is important: Companies buy fire insurance because they might lose their business if a fire occurs. The same holds true for companies that handle sensitive data, such as personal information.”

From the Report on Patient Privacy, Volume 11, Number 1: January 2011; Available online at www.aishealth.com

“There is no such thing as perfect security. Companies can throw large amounts of money at an attempt to build ‘Fort Knox,’ but they may still be breached,” he says. “So they have a choice: They can retain the risk or they can transfer the risk. Insurance is one way to transfer that risk, and after a certain point it might make economic sense for a company to do so — rather than invest more money in trying to achieve perfect security, which is impossible.”

Privacy and outsourcing attorney John Nicholson is also among those who recommend that his clients purchase cyber liability insurance. But he adds that every organization should also insist that others with whom they do business (other CEs [covered entities], BAs [business associates], subcontractors, agents, etc.) also have such insurance.

“You should require your suppliers to carry an appropriate level of insurance for the risk they create for you, but you don’t want to push all of your risk onto them,” says Nicholson, counsel with Pillsbury Winthrop Shaw Pittman LLP, in Washington, D.C. “Your suppliers will pass the cost of their insurance through to you in their charges, so if you force them to acquire too much insurance, then you’re going to overpay for the coverage.”

Process Begins With Risk Assessment

Many CEs and BAs have no idea where to start when considering a cyber insurance policy. A good first step is to check with the broker that provides other coverage. In Geney’s case, she worked with Charley Malmquist, president of Potter Holden & Co. of Atlanta.

Malmquist tells RPP he’s had a 300% increase in requests for cyber insurance quotes just this year, which he attributes to CEs and BAs coming to grips with the increased penalties for violations that were put in place with the HITECH Act.

Insurance Not a Substitute for Safeguards

“All the safeguards you can have are wonderful, and the insurance is not a substitute for those,” he says. But his clients “are beginning to understand their exposure and they are beginning to think maybe there is a different strategy rather than to self-insure for the exposure” that might result from a data breach. Before obtaining the policy, Malmquist has entities go through a risk assessment checklist on paper. This is used for underwriting purposes, to “make sure certain basic safeguards are in place,” Malmquist says. But it also “helps the clients in their self-evaluation.”

After initiating this process, some health care organizations have asked for assistance in beefing up their compliance and for help in locating resources for best practices, he adds. But there have also been some that simply never sent in a completed application.

When that happens, Malmquist has discovered it was because some just didn’t have the necessary safeguards in place. “There has been a reluctance to admit that they were noncompliant,” he says.

Malmquist says that about a third of clients “would admit to me that they felt the application was good for them” in terms of identifying compliance gaps.

If after reviewing the application, an insurer “feels there is not an adequate level of protection” the firm might decline to issue a policy or will increase the premium or possibly the deductible, or both, Malmquist says.

From the Report on Patient Privacy, Volume 11, Number 1: January 2011; Available online at www.aishealth.com

Group Bought \$1 Million Policy

How much coverage is needed? In Hemophilia of Georgia's case, officials determined that with its client base of 1,400, the lowest level of coverage — \$1 million — was probably sufficient. It chose to not purchase the two optional products that cover web-related issues and cyber extortion.

The organization's nurses and social workers provide services to clients in their homes, and have access to protected health information. In addition, HIPAA regulations also come into play in the organization's pharmacy sales and fundraising activities.

Security practices include a one-minute automatic logout on laptops, five minutes on desktops and mandatory encryption. Hemophilia of Georgia also pays for an external organization to conduct a security audit on a yearly or every-two-year basis. "Our auditor told us we are doing everything we should be doing," Geney says.

The \$1 million privacy and network liability policy Geney's organization bought cost \$9,000 in annual premiums and carries a \$25,000 deductible. Policies can go as high as \$5 million in coverage, with deductibles escalating to \$50,000. The policy Geney got has three coverage areas, and each has limits on what can be paid for what kind of cost or loss.

"We struck out the Internet section because that was a separate coverage and would greatly increase the premium," Geney said. "We believe we can get that somewhere else more cheaply based on what we need it for."

ACE, which insures the hemophilia organization, is among the "big players" in the cyber-insurance industry, according to Navetta; others are Chartis, Beazley, and Hiscox, he says. Malmquist says other firms that have a large presence are CNA and Allied World Assurance Co. of Philadelphia.

Variety of Firms Offer Coverage

"Many carriers now offer the coverage, and coverage is now more readily available in the smaller and middle markets," Navetta adds. In addition, many larger, full-service insurers have gotten into the business, including Travelers and the Hartford.

Some carriers may provide a cyber insurance endorsement to an errors-and-omissions or commercial general liability policy. Some are "very limited, like \$25,000 or \$50,000," Malmquist says. "In the event a loss occurred, that could give you a false sense of security," he adds.

Asked if a rider on a standard policy would be sufficient, Navetta responds that "in my view it is more important to get the right coverage. It matters less whether it is a standalone policy or an endorsement to an existing policy," he says. "However, it is probably a good question for a company to ask its broker. If the right coverage exists as an endorsement to an existing form, then it would be great to have it all combined."

In Navetta's view, all health care entities, including hospitals, and business associates, should now be "seriously considering" such insurance.

From the Report on Patient Privacy, Volume 11, Number 1: January 2011; Available online at www.aishealth.com

Breach Costs Can Be Very High

“Data security breaches can be devastating to an organization in terms of money spent to address the breach, especially for smaller and mid-sized organizations,” Navetta says. “There is a multiplier effect that can have a serious impact. If 10,000 or 100,000 or 1 million — or more — records are lost, in order to provide notice as required by breach notice laws, as well as credit monitoring and call center services, which may not be required by law, but which most companies provide after a breach, there may be a ‘per record’ cost.”

Some estimates put that cost at \$20 per lost record, an amount Navetta termed “conservative.” A large breach could cost from \$200,000 to \$2 million. “The situation might be worse if credit card numbers are involved and fraud has occurred or banks have to reissue credit cards,” Navetta says.

“Another benefit of the insurance is that the carriers have often pre-negotiated bulk rates for mailing costs, credit monitoring and call center expenses,” he says. Without such insurance, “if a company goes out into the open market after a breach, they are going to be at the mercy of the vendors in terms of price,” Navetta says.

Insurance Is a Cost-Benefit Decision

“Ultimately,” he adds, “the decision to purchase insurance is a risk management and cost-benefit decision.” CEs and BAs need to weigh the price of insurance “against the likelihood of a security or privacy breach occurring, and the potential impact to the organization,” he says.

Even organizations that are convinced of the merits of a cyber liability policy might be waiting to purchase one. Geney, who urges organizations to not wait, is concerned that premiums might become unaffordable in the future.

“If everyone starts making claims, then the price will go up,” Geney says. But she notes that so many of the best-known cases of HIPAA privacy and security violations seem to involve simple errors and oversights. “I don’t know that the policies cover stupidity,” she jokes.

From the Report on Patient Privacy, Volume 11, Number 1: January 2011; Available online at www.aishealth.com