

Malpractice Insurance Expert Advice

Cyber Liability 101

By Bill Gompers



Cyber liability is the risk posed by conducting business over the Internet, over other networks, or using electronic storage technology. Exposures are generally classified as a “first-party” or a “third-party” cyber liability. A “first-party” cyber liability occurs when your own information is breached. A “third-

party” cyber liability occurs when customer or partner information your organization has promised to keep safe is breached.

Healthcare organizations have access to sensitive patient and employee information including medical records, Social Security information, and other personal information, placing them at high risk for data breaches. According to the Ponemon Institute and the Privacy Rights Clearinghouse:

- Healthcare organizations account for one-third of all data security breaches reported across all industry segments nationwide.
- Insider actions (negligence or intentional acts) cause three times as many breaches as external attacks, such as hacking.
- Half of all insider actions nationwide, across all industries, occur in the healthcare industry segment.
- Healthcare organizations account for 25% of the approximately 30 million records exposed nationwide across all industry segments.
- The cost of a healthcare data breach averages \$214 per record, compared to \$194 per record for all industry segments combined.
- Almost half of all healthcare breaches result from lost or stolen laptops or other mobile devices.

In response to this expanding exposure, carriers have developed a cadre of standalone and add-on products to address the healthcare industry’s needs. Insurance companies have created programs and security strategies designed to mitigate both the first- and third-party risks caused by cyber liability. Although these policies are designed to provide protection and coverage for first- and third-party cyber liability exposures, none of the policies are identical in coverage and there is a lack of standardization in the terminology, coverage, and terms and conditions. Components of these products can include network asset protection, network security and privacy insurance, cyber extortion and terrorism coverage, and regulatory insurance.

With the increased emphasis on the enforcement of the myriad of laws directly and indirectly affecting data breaches by healthcare providers, it is prudent to have your cyber liability exposure reviewed and evaluate whether you have adequate coverage or reserves. This assessment can best be accomplished with the assistance of an experienced insurance broker who has expertise in healthcare providers’ malpractice risk.

Bill Gompers is a medical malpractice insurance specialist with Danna-Gracey, a state-wide independent insurance agency dedicated solely to insurance coverage placement for Florida’s doctors and healthcare providers, including medical malpractice, workers’ compensation, physician and employee benefits, and PEO (Professional Employer Organization) services. To contact him call (888) 777-7173, or e-mail bill@dannagracey.com.