Cyber Liability: Privacy & Data Breach Endorsement

A laptop is missing, customers’ payment records are stolen, paper files are lost, your website or network is hacked...Is your clinic prepared for a breach?

This CVMA program enhancement is your first line of defense in data breach preparedness, compliance and resolution. Count on us to deliver swift and thorough solutions to help protect and restore your business’ reputation and client’s trust.

KEY PROGRAM BENEFITS

• Endorsement to the General Liability Policy
• Affordable solution for Privacy Breach Coverage
• Combines 3rd party liability and expense coverage in a comprehensive package
• No deductible
• Access to our IDT911 Data Breach services

COVERAGE AT A GLANCE

PRIVACY BREACH LIABILITY
• Limit of $1,000,000
• Coverage for a data/privacy breach resulting in lost personal and protected information that affects your clients

INCLUDES PRIVACY BREACH EXPENSE:
• Limit of $25,000 with an option to increase to 50,000 or 100,000
• Crisis Management Expenses such as hiring a public relations advisor
• Credit Monitoring and Data Recovery for your clients
• Cyber Investigation Expenses to figure out how and when the breach occurred

DATA BREACH SERVICES

CVMA policy holders will also have access to breach preparation and crisis management services provided by IDT911. This includes access to an exclusive website with tips and resources on how to prepare for a data breach, along with personalized assistance on how to notify clients, and comply with privacy law in the event of a loss.
The Loss:
A merchandise distributor that does online sales, was in the process of transferring its data and redesigned website to a new host, when the old website was hacked. Hackers gained access to nearly 30,000 credit card numbers dating back five years. The merchant needed to inform its customers of the breach.

How the Policy Responds:
Card numbers were filtered to determine that 12,000 were still active. Notification letters were sent out to their customers, and fraud resolution was setup to offer further support.

The Loss:
A publicly traded company became a little too public when it unwittingly posted the personal information of several top executives online. Protected Personal Information (PPI) including social security numbers of the company’s top brass were accessible to anyone who visited the company’s website for four to six weeks.

How the Policy Responds:
The website logs were investigated to see how many visitors there were during the defined time period, and the executive’s bank accounts were put on fraud alert and were provided with credit monitoring.

The Loss:
An employee at a small accounting firm took home her office laptop to do some work over the weekend. An ill-fated stop at the mall left her with a broken car window, a stolen laptop and exposure more than 120,000 personal records. Her firm had been helping several large hospitals with their audits, and their patient’s protected health information (PHI; including prescriptions, procedures, and diagnostic codes) was only a password away from the thieves.

How the Policy Responds:
The level of protection of the computers were assessed. To comply with privacy law, all hospitals and 120,000 patients were notified. As the assessment and notification services were promptly completed, the accounting firm was able to stay in business.