

## CYBER SECURITY AND PRIVACY BREACH RESPONSE COVERAGE

An ever-increasing number of professionals are utilizing technology to communicate with patients and deliver their services. One of the consequences of tele-practice is an increase in cyber insurance claims, including those related to ransomware, social engineering, and other cyberattacks.

BMS recommends that professionals who are responsible for maintaining and safeguarding confidential information consider purchasing Cyber Security and Privacy Liability insurance to address their increased risk and exposure.

Should you or your business experience a cyber incident, in addition to coverage, this policy provides access to a Breach Response team who will assist with any necessary investigation and response services, which includes notifying impacted individuals.

### Consider a few examples where a Cyber Security & Privacy Liability policy may respond:

You open an attachment in an email from what you think is a trusted source. The attachment downloads malware to your computer, exposing your passwords, patient profiles, and other sensitive data.

You are walking to your car with a folder of files containing personal patient information and a gust of wind blows the files away, with no chance of recovery. Even though the files were not distributed digitally, confidential information has been breached.

An impersonator pretending to be your manager sends you an email asking for a password. You provide the information and have now given them access to your network.

### Fraudulent Instruction (optional addition to policy):

You receive an email from a supposed vendor advising that their wire payment information has changed. You update the information and make payments, then later hear from the actual vendor that they haven't received any transfers.

*This brochure is a summary of coverage and is for information purposes only. Full terms and conditions of the policy, including all exclusions and limitations are described in the policy wordings, a copy of which can be obtained from BMS Canada Risk Services Ltd. (BMS). For more information on the coverage please contact us.*

### Coverage Highlights

<b>Breach Response</b>	\$250,000
Legal, Forensic & Public Relations/Crisis Management	5,000 (Individual) 100,000 (Business)
Notified Individuals	
<b>Policy Aggregate Limit</b>	\$1,000,000
<b>First Party Loss</b>	
Business Interruption	\$25,000
Cyber Extortion Loss	\$100,000
Data Recovery Costs	\$100,000
<b>Liability</b>	
Data & Network Liability	\$1,000,000
Regulatory Defense & Penalties	\$250,000
Payment Card Liabilities & Costs	\$1,000,000
Media Liability	\$1,000,000
<b>eCrime (Optional)</b>	
<b>Fraudulent Instruction &amp; Funds Transfer Fraud</b>	\$25,000 & \$100,000 limits available for additional premium
The Fraudulent Instruction Endorsement provides coverage for loss resulting directly from the Insured having transferred, paid, or delivered money as a direct result of fraudulent instructions.	
Telecommunications Fraud	\$100,000
<b>Criminal Reward</b>	
Criminal Reward cover	\$25,000
<b>Deductibles</b>	
Each Incident	\$1,000
Notified Individuals	100

### How to Apply

Please visit [www.cao.bmsgroup.com](http://www.cao.bmsgroup.com) or contact BMS to purchase coverage.

#### BMS Canada Risk Services Ltd (BMS)

825 Exhibition Way, Suite 209  
Ottawa, ON K1S 5J3

Toll Free: 1-844-517-1371

Email: [cao.insurance@bmsgroup.com](mailto:cao.insurance@bmsgroup.com)

Web: [www.cao.bmsgroup.com](http://www.cao.bmsgroup.com)