Corvus Insurance
Smart Cyber Insurance®

Why Buy Cyber Liability?

10 REASONS HEALTHCARE ENTITIES NEED COVERAGE

1 | PRIVACY LAWS
Federal laws including the Health Insurance Portability and Accountability Act ("HIPAA") and the Health Information Technology for Economic and Clinical Health ("HITECH") Act require prompt notification if protected health information (PHI) that is not encrypted is lost, stolen or disclosed. These notification laws apply both to the "Covered Entity" itself as well to "Business Associates" of the healthcare organization. Cyber insurance will pay for investigators to identify the source and extent of a breach, attorneys to determine whether notification is required and draft the necessary letters, and breach response specialists to provide notification and credit monitoring services to affected individuals.

2 | BUSINESS ASSOCIATES
As noted above, HIPAA and the HITECH Act apply to Business Associates of a healthcare organization,
which are third parties that provide certain functions to the organization involving use or disclosure of PHI. According to the 2013 Redspin Report, 57% of all breaches in the healthcare industry involved a Business Associate. Business Associates do not have a statutory requirement to notify patients, only the "Covered Entity" has that obligation. Cyber coverage will pay for notification expenses even if the breach occurred while PHI was in the hands of a Business Associate.

3 |FINES/PENALTIES
Failure to comply with a privacy law can lead to significant fines or penalties. The Office of Civil Rights ("OCR"), which is charged with enforcing HIPAA, has made enforcing data privacy laws one of its top priorities. The OCR has received over 125,000 complaints of possible HIPAA privacy violations, and has brought thousands of enforcement actions resulting in a total of $28 million in civil fines. Cyber coverage can pay for the defense of these types of regulatory enforcement actions and the payment of any resulting fines or penalties.

4 | DATA DESTRUCTION
Hackers or rogue employees can destroy or damage a professional's electronic records, including customer lists, computer-aided files, and other critical materials. Cyber coverage will pay for the costs to restore or recreate these electronic records.

5 | SHUTDOWN
Cyber-attacks can disable, corrupt or shut down a construction professional's computer network preventing any work to be done and resulting in a shutdown of operations and consequential lost profits. Cyber coverage can pay for the loss of profits while these systems are down awaiting restoration.

6 | EXTORTION
Hackers can threaten to steal or disclose data, encrypt a company's entire network, or wreak other havoc on a business's computer network if a ransom is not paid. Cyber coverage can pay for the cost of the ransom to end the threat.

7 | CONTRACTS
Increasingly, professional firms are required to carry cyber liability insurance to meet bank, government and client contractual obligations. Cyber coverage can satisfy this requirement.

8 | CORPORATE INFORMATION
Healthcare firms often handle tremendous confidential corporate information. If this information, whether in paper or electronic form, is lost or stolen, a Cyber policy will protect the firm if sued by a client or a third party for failure to protect its confidentiality.

9 | REPUTATION
A firm's reputation in the community is among its most important assets. Public relations experts can help maintain the firm's reputation if a data breach goes public. Cyber coverage will pay for their services.

10 | BUSINESS ASSOCIATES/ VENDORS/STORAGE PROVIDERS
Your organization may transfer or entrust their data to business associates and vendors such as cloud storage companies, document storage or destruction providers, subcontractors or other third parties. In such situations, the firms remain responsible for safeguarding that data. If these third parties experience a breach, the firm, as the data owner, is responsible to provide notice to the affected individuals under most privacy laws. Cyber coverage will provide coverage, regardless of who caused the breach or where the data resided at the time of the compromise.

CYBER CLAIMS SCENARIOS - HEALTHCARE

Coverage: Cyber Extortion and Ransomware Coverage

- **A small medical practice** experienced a network breach caused by an email phishing scheme. All patient files held within the practice's servers were immediately encrypted by malware and the perpetrator threatened to delete all files until a ransom was paid out. The ransom, IT forensic costs, and legal expenses were covered by the practice's cyber liability insurance policy.

Coverage: System Failure Coverage

- **A large medical group** was investigated after a programming error within its computer system allowed the patient information of approximately 10,000 to become publicly visible on the internet. Cyber coverage made sure that patient notification services, IT forensics and legal expenses were paid for.

Coverage: PCI DSS Assessment

- **Over two thousand debit and credit card holders** found that their personal data had been exposed when card readers at several locations belonging to a nationwide medical group were compromised. An employee had attached 'skimming' devices to the readers and then sold the information on the black market. Because the group failed to maintain proper data security controls, fines and assessment were imposed.