Assurance4You

June 2016

What is Cyber Liability and Breach of Patient Data Privacy?

A data beach is the release of secure information into an unsecure environment. This happens intentionally or unintentionally. A data breach or security incident occurs when confidential data such as patient records, or personal financial data is copied, transmitted, viewed, stolen, or used by an individual unauthorized to handle such information.

This may involve information such as financial records, credit card, debit card, bank details, personal health information (PHI), personally identifiable information (PII), trade secrets, and intellectual property. Such incidents pose the risk of identity theft or other serious consequences.

Data breach is a growing concern across the world with the sophistication of criminal technological access, and the increasing technological legal access to records storage and transmission by honest people at work for professional use and at home for personal use.

The nonprofit consumer organization Privacy Rights Clearinghouse, identified over 227 million individual records that contained sensitive personal information that were involved in security breaches in the U.S. during the period 2005 through 2008.

Today's technology driven world has increasing risks associated with doing business online and storing sensitive data on paper and electronically. This has spawned the need for healthcare professionals to shift the risk to insurance carriers. For example, in 2005, fewer than 30% of businesses surveyed by the FBI had cyber liability insurance coverage. ***Today over 60% of businesses have some sort of cyber liability insurance coverage.***

The Federal government and many states have enacted laws with safeguards, notification requirements, and penalties to protect the security and confidentiality of information, and specifically medical information, as it is stored conventionally, electronically, and shared electronically.

An example of this aimed directly at the healthcare professionals began in March 2013, when Congress passed the 45 CFR Part 160 HIPAA HITECH Law which became enforceable on many occupations including social workers and the behavioral health industry effective September 2013.

This makes healthcare professionals liable for data privacy breach by third-party data management vendors used by them.

Under HIPAA, and in many states under state law, the healthcare professional is now ultimately responsible for protecting the client data no matter where the data is. The healthcare professional has this duty and is liable if the client data is compromised.

This includes third-parties who the healthcare professional hires to manage client records that become breached. This opens up many liabilities for the

healthcare professional in today's technology driven world.

The risks associated with doing business online and storing sensitive information electronically and on paper are increasing.

Data breaches now affect hundreds of millions of records each year. In 2013, the Computer Security Institute survey of 351 security professionals found that half of the respondents experienced at least one data security incident in 2012, and about 55% were accidental untargeted breaches.

Simply losing a laptop, a mover losing a records file box or an envelope with a patient file in it, a burglar simply opening up a file drawer in the healthcare professional's office, a lost flash drive, or the data management vendor accidentally faxing or emailing a patient record or form to the wrong phone number or email address, as well as a deliberate cyber attack on the data management vendor are all examples of data breaches which become the healthcare professional's responsibility.

As A Healthcare Professional – How Can I Get Protected?

Cyber Liability insurance coverage for small practices and social service agencies is still relatively new to the insurance world. Except for the NASW Risk Retention Group, virtually no insurance carriers have it as an affordable insurance addition for healthcare professionals. Those few carriers who do offer Cyber Liability insurance policies for Healthcare Professionals only offer it to Social Service Agencies and charge very high premiums.

Some Professional Liability insurance policies provide data breach coverage if the breach occurs within the control of the practitioner only. The NASW Risk Retention Group provides Professional Liability insurance protection that covers data breach within the control of the practitioner.

Now, the NASW ASI Risk Retention Group also provides a new Cyber Liability and Breach of Patient Data Privacy insurance policy that protects the practitioner from many other breach occurrences including Security Breach, Damages, Civil Monetary Penalties, and Defense Expenses.

This policy covers sole practitioners or individuals at the state and federal levels for third-party liability, including damages and civil monetary penalties the insured is legally obligated to pay and defense costs, arising from security breaches involving the personal information of the insured's patients if a breach occurs while the information is in the care, custody, or control of a third party to whom the insured has entrusted the information.

Such third-party includes a cloud vendor, a university whose computer system the insured uses to store records, a moving company hired by the insured to move the insured's office contents including records and equipment, or a records disposal company hired to destroy old records.

Coverage applies to electronic and paper records. It is an excellent cover for HIPAA HITECH protection arising from 45 CFR Part 160 which holds the social worker liable for data security breaches caused by third-parties that the healthcare professional uses.

This cyber liability policy covers:

a. reasonable costs to notify affected individuals and provides a one year subscription reimbursement benefit for identity theft protection,

b. legal defense costs if a claim is made against the insured by affected individuals or if a state or federal regulator brings a civil action against the insured,

c. damages that the insured is legally obligated to pay under court judgment or out-of-pocket court settlement, and any civil fines or penalties that the insured must pay because of the breach, and

d. the costs incurred for the insured to notify the insured's patients that data breach occurred.

This Cyber Liability policy is an excellent value for healthcare professionals. It provides a broad array of coverage and responds to recent data privacy legislation enacted by the Federal government and adopted by some states, and provides excellent coverage at extremely affordable premium prices.

Healthcare Professionals now, more than ever, need insurance coverage for third-party data breach. Federal and State governments demand higher expectations from Healthcare Professionals, and with the advent of the HIPAA HIGH TECH Law, they are held liable and even more accountable than ever before.

Assurance4You is part of the NASW Risk Retention Group, Inc. product suite. Coverage is provided by the NASW Risk Retention Group, Inc