Cyber Liability: Laptop Theft and Other PHI Breach Risks

written by CPH Insurance | November 22, 2017

Published November 22, 2017

Cyber risk: we've all heard about it. It's making headlines nationwide with large companies such as Target[1] and Equifax[2] suffering massive data breaches. Though we often don't hear about it in the mental or allied health industries, it doesn't mean that breaches aren't happening. If you think about it, allied and mental health care providers—especially business entities[3]—are often at *greater* risk given the large amount of sensitive patient records they hold.

CPH & Associates is proud to offer cyber liability coverage to our mental and allied health policyholders (both individuals and business entities) to help our customers address their cyber risk concerns. When considering coverage as an allied or mental health care provider, you'll want to make sure it protects against breaches of PHI (Protected Health Information). This is one key facet of CPH & Associates' cyber security liability coverage. See below for a more detailed description:

> Breaches of PHI (Protected Health Information): Defined under HIPAA (Health Insurance Portability and Accountability Act), PHI includes any medical record (electronic, written or oral) that can individually identify a patient. Examples include billing information, diagnoses, visit/referral notes, test results, prescription information, scheduling communications, or any other personally identifiable information used or disclosed by a provider during the course of care. HIPAA's Privacy and Security Rules require that "covered entities" (those that are covered by HIPAA, including all healthcare providers, insurers, etc.) maintain reasonable and appropriate administrative, technical, and physical safeguards to protect medical records. Any breach of PHI requires notification to the Department of Health and Human Services' Office for Civil Rights (OCR), which has broad authority to investigate breaches, require corrective action, and/or reach monetary settlements (a type of regulatory fine) with covered entities found to be out of compliance with the regulation. In addition to the OCR, 48 states have their own breach notification laws which require timely investigation and notification of any such breach to the state's affected residents – these laws are enforced by the state attorneys general.

"Realistically, though, can this happen to me?" Yes it can. Here are just a few more recent examples of data breaches specifically affecting mental and allied health professionals:

1. Thousands of patient records in New York were leaked from a New York hospital this year[4] due

to a cyber security breach, exposing medical diagnoses, HIV status' and reports of sexual abuse and domestic violence. *(Referenced article published May 2017)*

2. In Maine, thousands of patient records were compromised in a cyber security breach[5] at a Behavioral Health Center, risking patient clinician notes and diagnoses, addresses, Social Security numbers and phone numbers. *(Referenced article published April 2017)* ***Please note: CPH & Associates does not offer professional liability insurance to psychiatrists.***
3. Hackers gained access to Burrell Behavioral Health Patient information[6] via a cyber security breach in Springfield, Missouri, compromising patient's names, addresses, Social Security numbers and even "protected" medical records. *(Referenced article published October 2016)*

Picture this:

> *A therapist accidentally leaves his laptop at a coffee shop, only to return later and discover it has been stolen. Contained on the laptop were 75 patient files from the past three years, including insurance information and session notes. Unfortunately, the laptop was not encrypted, so the therapist's attorney determines that this constitutes a reportable breach of PHI. The OCR is notified of the breach, along with the state Attorney General. Breach notifications must be mailed to all affected patients and credit monitoring services are offered in accordance with statutory requirements. Although no further regulatory action is taken, the therapists total expenses (legal, notification, credit monitoring) are $15,000, which is covered under the Security Event Costs portion of his policy.*

Whether caused by hackers or simple human error, data breaches are a real threat to professionals in the mental health field. Consider protecting yourself from these increasingly prevalent—and costly—privacy events by adding Cyber Liability coverage to your Professional Liability policy. For detailed information about Cyber Liability cost & coverage amounts offered by CPH & Associates, click here!

Please note: Cyber liability is NOT a stand alone insurance policy offered by CPH & Associates. To take advantage of cyber liability, you will need to have a mental / allied health malpractice insurance policy through CPH & Associates and add cyber liability onto that policy. Additionally, cyber liability is designed to protect digital privacy of your client's information and DOES NOT cover loss of personal property. For Personal Property coverage, please inquire about CPH TOP which includes General Liability AND Personal Property coverage as an extension to your professional liability.

***As of May 2022, cyber liability is NOT currently available in the following states: Alaska and will never be offered to the states of North Dakota and New Mexico.**

References:

1. Finkle, Jim. Skariachan, Dhanya. “Target cyber breach hits 40 million payment cards at holiday peak.” Web blog post. *Business News*. Reuters, 18 December 2013. https://www.reuters.com/article/us-target-breach/target-cyber-breach-hits-40-million-payment-cards-at-holiday-peak-idUSBRE9BH1GX20131219 accessed on 10/13/2017
2. McCrank, John. “Equifax says systems not compromised in latest cyber scare.” Web blog post. *Cyber Risk*. Reuters, 12 October 2017. https://www.reuters.com/article/us-equifax-breach/equifax-says-systems-not-compromised-in-latest-cyber-scare-idUSKBN1CH2F3 accessed on 10/13/2017
3. Borowicz, Stacey A. White, Courtney M. “Cyber-Attack Response Guidance for Covered Entities and Business Associates.” Web blog post. *Legal News*. The National Law Review, 14 September 2017. https://www.natlawreview.com/article/cyber-attack-response-guidance-covered-entities-and-business-associates accessed on 10/13/2017
4. O’Hara, Mary Emily. “Thousands of Patient Records Leaked in New York Hospital Data Breach.” Web blog post. *News*. NBC News, 10 May 2017. https://www.nbcnews.com/news/us-news/thousands-patient-records-leaked-hospital-data-breach-n756981 accessed on 10/13/2017
5. Farwell, Jackie. “More than 4,000 patients at risk in hacking of Bangor psychiatric center.” Web blog post. *Bangor*. BDN Maine, 25 April 2017. http://bangordailynews.com/2017/04/25/news/bangor/more-than-4000-patients-at-risk-in-hacking-of-bangor-psychiatric-center/ accessed on 10/13/2017
6. Elzie, Sheena. “Hackers gain access to information of Burrell Behavioral Health patients.” Web blog post. *KSPR News.* ABC KSPR 33, 18 October 2016. http://www.kspr.com/content/news/Hackers-breach-security-of-Springfields-Burrell-Behavorial-Health-patients-397473361.html accessed on 10/13/2017