Insurance Coverage, Breaches of Confidentiality and HIPAA

By Pamela J. Van Cott, CPCU, Assistant Vice President, American Professional Agency, Inc.

We have passed the 20 year mark since HIPAA has been a part of our lives. The more recent HITEC Act/Omnibus Final Rule legislation, enacted in 2013, expanded the universe of who must be compliant, greatly narrowed the possibilities of providers avoiding the costs related to breaches and substantially increased penalties. A provider can now be responsible for the actions of business associates who are not HIPAA compliant. Another change relates to what now constitutes a breach. Previously, there was a need to find that "harm" was done to a client as a result of a breach of privacy. Now a breach just needs to be in violation of these more stringent rules to result in fines and the additional costs that comes with notification and remedy. Though violations can range from the unintended oversight to the truly outrageous, the costs for even the most unintentional and accidental of violations can be substantial.

So if one is suddenly faced with the knowledge that a breach has occurred, what type of insurance can help with the resulting expenses?

Here are a few scenarios of unintended harm on the part an individual counselor or health care facility to illustrate the actions that can be taken against them, by whom, and how an insurance policy may respond:

- A business laptop is lost or stolen;
- A retiring health professional closes his practice and entrusts his records to a third party who disposes of the records by leaving them curbside;
- A healthcare provider uses a third party to provide billing services and hackers get into the billing company's records, gathering information about the providers' clients resulting in identity theft;
- An employee of a health care facility posts private information about a client and the client's diagnosis to a social media site;
- A leased fax/copier machine is returned to the vendor, with all transmittal information about their clients still on the hard drive.

In these scenarios, the health care provider may be facing at least two separate sources of concern:

- **Risk exposure from unhappy clients:** Clients can suffer emotional distress and mental anguish should personal health information become public. Clients) may also suffer ensuing financial loss if the breach leads to identity theft or the loss of a job.
- **Risk exposure from National (HIPAA) or state regulators:** Regulators will investigate to see if a violation of their standards led to the breach. Individual counselors who sought exemption from compliance with HIPAA standards are still expected to be in compliance with their state privacy laws. HIPAA and other regulators do not bring lawsuits; they set standards. Violations of HIPAA standards are investigated by the Office for Civil Rights (OCR), a division of the U.S. Department of Health and Human Services, who has the power to investigate and, based upon their findings, levy fines while working with the facility to remedy the harm.

What type of insurance policy may respond to a lawsuit arising from an unhappy client?

When a client discovers that personal information has been made public due to the negligence of their healthcare provider, the main remedy available to them if they feel they have been injured, is to bring a lawsuit against the parties they feel were responsible. The allegations may allege emotional distress/mental anguish or the potentially more damaging allegation of financial injury, especially if the breach resulted in identity theft. A covered claim will be defended by an insurance company, and the plaintiff will have to demonstrate not only that a wrongful act did occur, but that he or she was injured by that act in order for a settlement or judgment to be paid by the insurance company.

Larger healthcare facilities will have one or more of the following types of liability coverage:

- General Liability
- Directors and Officers Liability
- Professional Liability specific to the healthcare industry
- Cyber Liability — This is still a relatively new insurance product with a wide variation of policy forms, limits and deductibles.

Many of these policies are not boilerplate policies, so coverage can vary, for example, between one healthcare facility's Professional Liability coverage and another's. In addition, the way a lawsuit's allegations are worded may determine what type of insurance policy will respond to defend the allegations and pay settlements or judgments. For almost all of these policies, criminal and deliberate acts of the insured that cause the most outrageous type of breach will be specifically excluded. A healthcare provider's insurance professional will work closely with their insured to determine

which policies may respond to a specific lawsuit and its allegations.

Individual counselors who are W-2 employees or 1099 contract workers for a larger facility may have coverage provided for them by their employer. If they are not knowledgeable about the scope of coverage being provided on their behalf, they should consider purchasing their own professional liability policy that will have their best interests in mind instead of relying on an employer's policy which has the employer's best interest in mind. Individual counselors who have their own professional liability policy will most likely have coverage for both defense and settlements/judgments for suits alleging breach of confidentiality. Professional liability for individual counselors are as varied as the number of insurance companies that provide this coverage, so counselors should inquire how their individual professional liability would respond if they are sued by a disgruntled client due to breach of confidentiality. A provider's professional liability policy that excludes coverage for HIPAA violations should still respond to a lawsuit brought by a client for breach of confidentiality.

What type of insurance policy may respond to penalties imposed by a regulator and other financial exposures related to a breach of confidentiality?

Regardless of whether or not an unhappy client brings suit against a health care provider, the provider may also have to respond to alleged violations of HIPAA or a state regulator's standards. All guidelines will require a provider to notify regulators as soon as they become aware of a breach. The quicker a breach is addressed, the better the chance to lessen the financial impact to the provider. Once a breach happens, here are some of expected costs that can be incurred due to a regulators investigation and findings:

- **Penalties and Fines:** HIPAA and/or state regulators can impose monetary penalties and fines. The maximum fine for HIPAA violations is currently $1.5 million for each violation.[1]
- **Other Costs of Data Breach:** The healthcare provider will need to notify patients/clients of a breach that may compromise protected healthcare information. There will also be costs associated with putting new security measures in place, hiring consultants to assist in response methods and the loss of revenue due to lost customers. Some healthcare providers may offer identity theft coverage to their clients for a period of time in order to re-establish good will. According to a 2015 report on the costs of a data breach, the healthcare industry has one of the highest costs to resolve a data breach, over $300 per patient.[2]

The policies that larger healthcare facilities have in place to defend them from lawsuits, (i.e. Directors & Officers Liability, General Liability and Professional Liability) may also include special wording that will broaden the policy to offer various levels of protection for the costs shown above. Though the primary purpose of these policies is to respond to *lawsuits* brought by parties that allege they were harmed due to an insured negligence, in recent years some insurance companies have broadened their policies to give a limited amount of coverage for additional costs that may result from a regulator's investigation. Some insurance policies have specific exclusions pertaining to HIPAA or state regulator violations. Generally, a separate limit will apply to actions brought by regulators, and the limit may be much lower than the full liability limits of the policy. Some policies may only cover fines and penalties while others will cover fines, penalties and the other costs incurred by the insured in notifying clients of a breach.

Many individual providers will only have a Professional Liability policy that protects the insureds for their negligent acts. Some of these policies now have a sublimit (e.g. $25,000) to protect the insured from a "Privacy Wrongful Act" claim brought by a "Regulator." Individual counselors should ask their insurance representative about the limits that may be available and the extent of coverage provided.

As stated earlier, a Cyber Liability policy is a relatively new insurance product that has become popular in the last several years as a result of the high profile cases of criminal hacking of healthcare facilities, retail chains and financial institutions. This type of policy will offer higher limits than may be available under more traditional policies. Both small and large healthcare providers may find greater peace of mind by purchasing this type of policy. According to the 2015 Ponemon Institute study, nearly 50% of all breaches are now due to hackers.[3] It cannot be assumed that small facilities have less exposure to cyber thefts than large facilities. Hackers know that larger facilities can afford a more sophisticated level of protection so they will often go after a softer target — the smaller facility with less cyber protection. Before purchasing this specialty coverage, check with your insurance representative to see what coverage is already provided under your other policies.

Of course, preventing a breach through risk management is the best way to avoid enduring the stress and cost of litigation and regulatory investigations. Most providers are already familiar with these prevention methods from the earliest years of HIPAA and other privacy laws, and more detailed security steps are widely available through an internet search:

- Establish written security and privacy policies, incident response plans and corrective action plans and review them routinely.
- Train all employees, provide document training, conduct reviews and be ready to enforce these policies.
- If using the cloud for storage, make sure your contracts with cloud providers does not make you responsible for breaches of your data.
- Delete media from devices that are no longer used, even fax/copier machines.
- Use the latest encryption technology for all computers and devices, including mobile phones.

Omnibus/HITECH legislation requires that the following additional risk management techniques be followed due to a provider's broader liability exposure for the acts of business partners or associates:

- Make sure you have written contracts with business associates that have been reviewed by an attorney that is familiar with HIPAA regulations. When possible, the business associate should add the provider as an additional insured.

Most importantly, act quickly to notify your insurance company immediately once a breach has been made known. Your policy mostly likely has provisions that require that the insurance carrier be notified before any notification or corrective action procedures are implemented by the provider. Avoid jeopardizing insurance coverage by complying with the terms of the policy that pertain to notification.

ENDNOTES

[1]American Recovery and Reinvestment Act, 42 U.S.C. § 1320d-5(2009).

[2]Ponemon Institute (2016). *Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data,* Ponemon Institute LLC. Retrieved at http://www.ponemon.org/library/sixth-annual-benchmark-study-on-privacy-security-of-healthcare-data-1.

[3]Ibid.

Pamela J. Van Cott, CPCU, is Assistant Vice President with the American Professional Agency, Inc. (APA, Inc.), NAADAC's partner and endorsed professional liability company. Van Cott has 25 years of experience insuring professional liability, with a concentration in the addiction field. APA, Inc. has been a leading writer of professional liability for mental health and other professionals for 40 years. With over 100,000 insureds, APA, Inc. has been endorsed or sponsored by many national and regional mental health associations, including NAADAC. In addition, APA, Inc. has experienced staff to provide risk management consultation services for policyholders.