Avoiding Malpractice
Tips for Social Workers to Manage Risks

July 2019

Because We Care, We Are Security Aware

Did you know that recently the City of Baltimore suffered a cyber attack that froze its ability to operate, including processing parking tickets?

In early June of 2019, Philadelphia's court system was attacked which froze its ability to operate. Cyber attacks span a wide variety of categories that cause disruption, steal money, extort money from victims, and/or steal information, usually to sell for identity theft purposes.

The NASW Risk Retention Group is the only insurance carrier in the nation that offers the lowest cost stand-alone insurance policy protection against cyber risks. We will discuss what this means to you and your practice in this article.

But first, here is a brief overview.

According to a 2017 insurance industry claims history study by Hanover Research/ Market Insight Center, "***Cyber Liability Insurance Market Trends: Survey***", the top five cyber related insurance claims that comprise 75% of all cyber liability insurance claims are:

25% Hacker

16% Malware Virus

12% Stolen Laptop/Device

10% Staff Mistake Records Disclosure

9% Paper records Breached

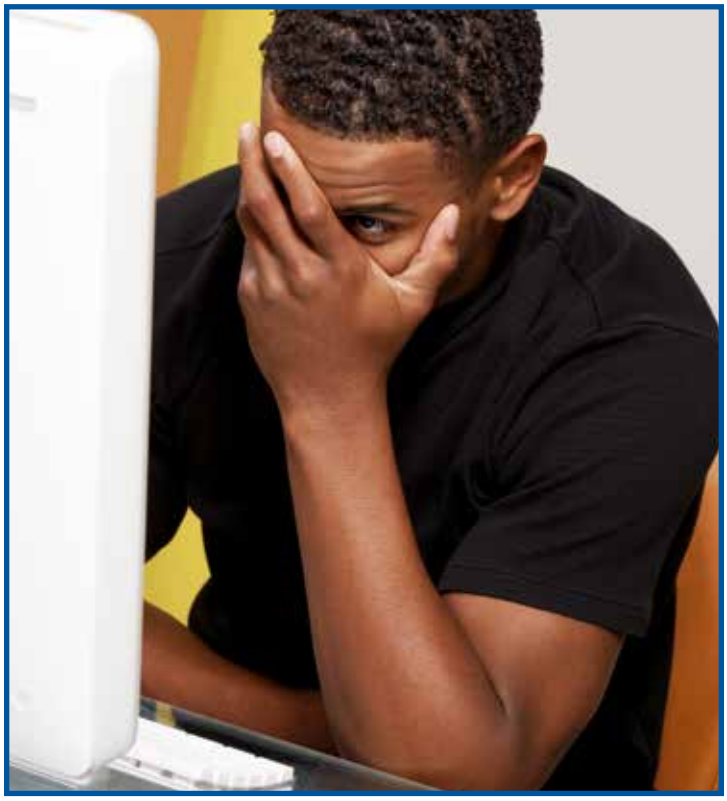
Our national insurance claims experience indicates that social workers and

Avoiding Malpractice is a publication of NASW Assurance Services, Inc.
as part of our mission to educate social workers on the benefits and importance of liability insurance.
For more information visit www.naswassurance.org.

behavioral health practitioners in general, are more susceptible to records breach risks and related insurance losses than to extortion risks or other cyber risks. While these losses may not be huge cash losses, there are HIPAA consequences and fines involved that will certainly cost the practitioner, and depending on the size of the breach could bankrupt the practice. More on that later in this article.

On the other hand, cyber criminals almost always seek money, so they target banks and credit unions for access to large customer information files, credit card issuers for credit card information that can be rapidly converted to cash and merchandise through retail transactions, and they extort money from large healthcare firms and large businesses. Most cyber criminals target potential victims for identity theft which include credit card theft because they are quickly and easily monetized and utilized for other purposes, frequently by overseas criminals.

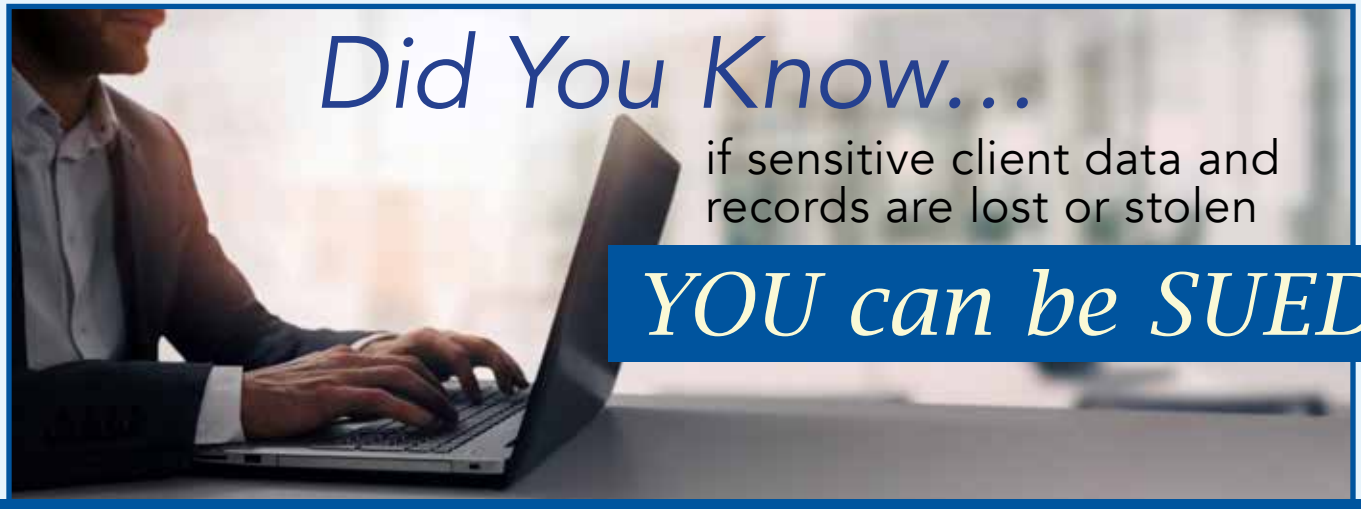
Some cyber-criminals cleverly intercept and control the health care organization's accounting records after a normal monthly accounting close where the records were unknowingly backed up to the cyber criminal's computer and routinely deleted as part of the monthly close procedure. Then the cyber criminal demands and extortion payments in exchange for file restoration. Restoration rarely occurs. This type of theft typically occurs to large practices with high volumes of billings and large organizational cash flow, such as cardiac surgical organizations for example. Almost always,



the records are not restored even after the ransom is paid.

Social workers and behavioral health practitioners are more susceptible to client records breaches, lost client files by third parties, and misdirected faxes. This places them squarely in the federal cross-hairs of the 45 CFR Part 160 HIPAA HITECH Law.

Records breach can occur from unauthorized access or exposure to a file cabinet containing a client's files, a mover (third-party breach), who loses your box of client files, a practitioner who sends a fax containing client information to the wrong phone number, or a cyber-criminal who breaks into your client records data base searching for information that can be monetized. The NASW Risk Retention Group



Did You Know...

if sensitive client data and records are lost or stolen

YOU can be SUED?

NASW does! Cyber Liability Protection safeguards your practice when storing sensitive client data electronically or liabilities associated with doing business online. It helps protect your practice against the costs associated with a security breach.

For More Information call 888-278-0038 or email asi@naswasi.org

Cyber Liability policy covers all of these claims for its policyholders.

Virtually all of the top cyber liability insurance claims require an attorney for the practitioner's legal defense. What does that mean to you? About $300 to $850 per hour, and most probably a $5,000 to $10,000 deposit paid in advance for starters for your legal defense.

So it makes a lot of sense to buy an NASW RRG cyber liability policy which starts at $59 per year for an NASW member. Non-members of NASW can also purchase cyber liability coverage for as low as $109 per year. We recently adjudicated a cyber liability claim for an NASW RRG insured with a total expenditure of $10,000. It involved a practitioner who thought a caller was a government representation and he revealed his user ID and password. The cyber-criminal entered the data base looking for financial information and credit card numbers, but none were on the file so damages were minimal. This was a small claim because there were no client damages and the client file size was modest. Nevertheless, $10,000 was the claim cost. If no NASW RRG cyber liability insurance coverage existed, then the practitioner would have paid $10,000 cash. The major costs arose from legal defense, security audit, and notification to the entire client base. The NASW RRG has no deductibles in any of its products.

The major cyber liability perils include legal defense, state and federal fines and penalties, damages to clients, the required security breach audit, client notification

costs, and the required ID theft protection subscriptions for victims.

The importance of Cyber Liability and Breach of Patient Privacy were heightened in September 2013 when the 45 CFR Part 160 HIPAA HITECH Law was launched. The practitioner is held ultimately responsible for protecting client information no matter where the data resides. This includes third-party movers handling your files, and data network cloud providers. In the event of a breach, this law requires the practitioner, YOU, to do the following:

1) Pay for a one-year identity theft subscription for each victim; (this costs more than the annual premium for an NASW RRG cyber liability policy);

2) Pay for a notice by letter to each, and every client in which the breach is described;

3) Pay for a mandated security audit by a recognized computer system auditing company;

4) Pay all state and federal fines and penalties;

5) Pay for your legal defense fees;

6) Pay for damages sustained by your client(s); and

7) Pay, or serve civil and criminal penalties that include $100 to $25,000 per occurrence, and up to $1.5 million for willful neglect. The criminal penalties range from 1 year in prison to 10 years in prison.

Now you are security aware.

Not all professional liability insurance policies cover patient records breaches, so read your policy carefully. The NASW RRG professional liability policy is the most comprehensive in the industry. The NASW RRG also offers a low-cost cyber liability policy that protects the practitioner against third-party information breach for which HIPAA holds the practitioner accountable.

Questions? Let's Discuss How We Can Help

Learn more about our Professional Liability Insurance for social workers by visiting www.naswassurance.org.

Our exclusive program is the only program endorsed by the National Association of Social Workers. To speak with a knowledgeable, licensed insurance representative, call 888-278-0038.

NASW™ Assurance Services
Where Social Workers Come First™