CyberAssurance COVERAGE

Underwritten by:

NAS insurance

PICA

Treated Fairly

Underwritten by a ProAssurance Company

(800) 251-5727 | www.picagroup.com

PICA Treated Fairly

Underwritten by a ProAssurance Company

CyberAssurance FOR HEALTHCARE

As more patient health information is stored and shared online, in email, and on mobile devices, there is greater risk of theft or exposure of that information by cyber criminals. Cyber criminals are smart and opportunistic. They look for the quickest way to get in, get information, and get out without being detected, and they always seem to be one step ahead. In addition, the government is increasing scrutiny of businesses' data security practices, potentially exposing you to significant fines and penalties should there be a breach.

Is YOUR practice cyber safe?

DID YOU KNOW?

- In 2016, Identity Theft Resource Center (ITRC) reported:[1]
  - The total number of cyber breaches among all sectors grew more than 40% from 2015.
  - The healthcare/medical sector ranked 2nd in the number of breaches reported (36.2%), and 1st in the number of records affected (43.8% of over 35 million records).
- Symantec reported a steady increase between 2010-2015 in cyber-attacks targeting businesses with less than 250 employees and found that 43% of all cyber-attacks in 2015 targeted small businesses.[2]

Ten Cyber Security Tips

- Train employees in security principles.
- Protect information, computers and networks from cyber-attacks.
- Provide firewall security for your Internet connection.
- Create a mobile device action plan.
- Make backup copies of important business data and information.
- Control physical access to your computers and create user accounts for each employee.
- Secure your Wi-Fi networks.
- Employ best practices on payment cards.
- Limit employee access to data and information; limit authority to install software.
- Require passwords and authentication.

INSURANCE HIGHLIGHTS

Your CyberAssurance endorsement includes access to online cyber risk management resources, tools to help you identify and mitigate cyber risks, and breach response services if you suspect that your practice has experienced a cyber breach.

Online Risk Management Website

- Compliance materials so you can analyze and adhere to state and federal compliance laws.
- Tips to help you actively implement best practices and preventative measures.
- Training courses, bulletins and webinars to generate cyber risk awareness among management and employees.
- Guidance for setting up a breach response plan to react quickly and efficiently.

Breach Response Services

- NAS Claims Specialists to coordinate the breach response team and assist the team throughout the process until the claim is resolved.
- NAS assigned legal counsel to act as "breach coach" - the point person who will coordinate all breach response activities on behalf of the Insured. If necessary, specialists may be engaged, and may include:
  - **IT security and forensic experts**
  - **Public relations/advertising support**
  - **Breach notification**
  - **Call center and website support**
  - **Credit monitoring and identity theft restoration services**

Sources:
1. Identity Theft Resource Center, "2016 Data Breach Report" ITRC Surveys & Studies, released January 18, 2017
2. Symantec, Internet Security Threat Report, Volume 21, April 2016, pages 45, 34-35 (accessed November 10, 2016)

PICA
Treated Fairly

Underwritten by a ProAssurance Company

CyberAssurance
COVERAGE SUMMARY

First Party Losses

- **Privacy Breach Response Costs, Patient Notification Expenses, and Patient Support and Credit Monitoring Expenses** – Coverage for reasonable mitigation costs and expenses incurred as a result of a privacy breach, security breach or adverse media report, including legal expenses, public relations expenses, advertising and IT forensic expenses, postage, and the cost to provide call centers, credit monitoring and identity theft assistance.
- **Network Asset Protection** – Coverage for amounts incurred to recover and/or replace electronic data that is compromised, damaged, lost, erased or corrupted due to (1) accidental damage or destruction of electronic media or computer hardware, (2) administrative or operational mistakes in the handling of electronic data, or (3) computer crime/attacks including malicious code and denial of service attacks. Coverage also extends to business income loss and interruption expenses incurred as a result of a total or partial interruption of the Insured's computer system directly caused by any of the above events.
- **Cyber Extortion** – Coverage for extortion expenses incurred and extortion monies paid as a direct result of a credible cyber extortion threat.
- **Cyber Terrorism** – Coverage for loss of business income and interruption expenses incurred as a direct result of a total or partial interruption of the Insured's computer system due to an act of cyber terrorism.

Liability Claims (Duty to Defend)

- **Multimedia Liability** – Coverage for third party claims alleging copyright/trademark infringement, libel, slander, plagiarism or personal injury resulting from dissemination of media material. Covers both electronic and non-electronic media material.
- **Security & Privacy Liability** – Coverage for third party claims alleging liability resulting from a security breach or privacy breach, including the Insured's failure to safeguard electronic or non-electronic confidential information, or the failure to prevent virus attacks, denial of service attacks or the transmission of malicious code from the Insured's computer system to the computer system of a third party.
- **Privacy Regulatory Defense and Penalties** – Coverage for regulatory fines and penalties and/or regulatory compensatory awards incurred in privacy regulatory proceedings/investigations brought against the Insured by federal, state, or local governmental agencies, such as proceedings/investigations alleging HIPAA violations.

PICA
Treated Fairly
Underwritten by a ProAssurance Company

CyberAssurance
RISK SCENARIOS

1. Multimedia Liability

A podiatrist used a photograph of a child to advertise podiatry services for youth on his website and Facebook page without obtaining parental consent. The parents of the child discovered the Insured's use of the image and asked that the image be removed.

Although the podiatrist complied with the request, an attorney for the parents sent a letter to the podiatrist demanding compensation for copyright infringement and unauthorized use of the photograph for advertising purposes. The case was resolved with a settlement $6,000. Legal fees cost an additional $8,500.

2. Security and Privacy Liability

An iPad issued to an employee of a podiatry group went missing. The iPad contained confidential records, including personally identifiable information (PII) and protected health information (PHI), of over 1,000 patients. The group notified affected parties of the breach and offered 12 months of credit monitoring.

Several weeks following the incident, the group was served with a lawsuit filed on behalf of several of the affected patients alleging failure to safeguard their confidential information. The cost to notify the affected patients and to offer credit monitoring exceeded $20,000.

3. Cyber Extortion

A podiatry practice had its network breached by an email phishing scheme when an unsuspecting office manager opened an attachment to an email that contained a ransomware virus. The virus encrypted patient files stored on the practice's servers, and the perpetrator threatened to delete all files unless a ransom was paid. The practice consulted with its cyber liability insurance carrier and retained legal counsel and an IT forensics specialist to investigate.

The IT forensics specialist determined the threat to be credible, and recommended that the ransom be paid so that further exposure and/or loss resulting from the incident could be assessed. Total costs and expenses came to $17,600 which included the ransom paid.

4. Privacy Breach Response Costs, Patient Notification Expenses, and Patient Support and Credit Monitoring Expenses

A programming error within the computer system at a large podiatry practice erroneously allowed patient information to become publicly visible on the internet.

There were approximately 8,700 patients affected by this breach. The costs associated with the breach included patient notification costs, IT forensic expenses, legal fees, and public relations expenses, all totaling more than $125,000.