PRIVACY//101℠

ALLIED WORLD ASSURANCE COMPANY

Healthcare Providers and Organizations have an obligation to keep people's information private.

When a patient, employee or client gives a healthcare provider or organization their name and other details including their health information, credit card number, social security number or bank account information or perhaps information on their financial position, they trust that it will protect this information. In fact, it is expected to do so as a matter of doing business.

The general public and their state representatives feel so strongly about this need for protection that at least 46 states have enacted legislation that requires a business or healthcare provider or organization to take action when it becomes aware that this information has been stolen, lost or subject to unauthorized access. Taking the appropriate action is costly. Failure to respond appropriately could result in the healthcare organization being fined by the states, sued by the individuals whose information was breached and, if made public, result in the loss of new or existing patients. The routine practice of accepting, maintaining or transmitting personal information creates both a responsibility and a financial exposure.

Consider these claims scenarios:

ROGUE EMPLOYEE: A problematic nurse finds out that he is about to be terminated and in response, 'cuts and pastes' health records that a healthcare organization holds on its patients to a public website. When its patients find out about this, they sue the healthcare organization for invasion of privacy and demand remediation.

PAPER FILES: Confidential paper files containing names and checking account information of donors are found in a dumpster in the organization's parking lot. The press gets a hold of the documents and publishes an article in the local newspaper. The organization needs to notify all affected donors and pay for advertising in the local newspaper. Identity theft hasn't been ruled out.

HACK/IDENTITY THEFT: An office computer network is hacked by a local teenager who steals social security numbers, bank account information and credit card numbers from an organization's patients and/or employees. He then sells the information to an Internet website which uses the information to create false identities for criminals to use. While there are notification and credit monitoring costs, the defense and damages resulting from potential lawsuits could easily bring costs into the hundreds of thousands of dollars.

One or more of these scenarios could apply to most, if not all, organizations, including healthcare providers and organizations. In fact since 2005, thousands of data breaches have been reported where a total of over 500 million individual records containing sensitive, personal information were exposed.* With the cost to provide credit monitoring to an individual whose record has been breached ranging between $20.00-$30.00/individual could most healthcare organizations afford these expenses if faced with a breach? What type of protection do they need?

We have the answer — PRIVACY//101.

WHAT IS PRIVACY//101?

Insurance that covers a business, healthcare organization or other organization in the event of a data breach involving lost or stolen information, whether paper or electronic.

WHO DOES PRIVACY//101 PROTECT?

Small to mid-sized companies or organizations that maintain employee or patient social security numbers, credit card details, bank account information, health information and other private information on less than 50,000 individuals with no claims or losses involving over 100 records.

WHAT DOES PRIVACY//101 DO?

Covers most costs associated with a privacy data breach including:

- Notification to all individuals whose private information may have been lost, stolen or accessed without proper authorization (notification is required in most states)
- Associated costs for those individuals electing credit monitoring in the event their information was lost, stolen or accessed without proper authorization
- Third Party financial claims and legal costs in the event of a suit and defense and penalty costs in the event of a regulatory claim (data breaches may be subject to state and federal penalties)
- Public relation expenses to protect and restore a company or organization's brand and public image
- Expenses to retain a data forensics expert to determine why the breach occurred and how to avoid one in the future

AVAILABLE LIMITS:

- Maximum Limit Options – up to $1M
- Pre-determined Retentions - Based On Industry and Revenues
- Minimum Premium - $300

WHAT ELSE?

- Privacy 101 insureds receive a ***Guide for Data Security Breach Preparedness and Response*** from our partner law firm Hogan Lovells, one of the largest and most experienced Privacy and Information Management practices in the world

JURISDICTIONS:

Privacy//101 is available in all 50 states on a surplus lines basis.

APPLICATION:

No new application to complete! Just send us annual revenues and the type of company.

FINANCIAL STRENGTH:

We believe that our "A (Excellent) XV" rating from A.M. Best, conservative balance sheet, expanding scope of operations and solid capital base put Allied World in a superior position to withstand future economic upheavals and to provide our insureds the protection they need.

* source: Privacy Rights Clearinghouse 2011

CONTACT INFORMATION

ALLIED WORLD ASSURANCE COMPANY (U.S.) INC.
199 Water Street
24th Floor
New York, NY 10038

Josh Ladeau
Tel: 860 284 1654
E: joshua.ladeau@awac.com

Adam Sills
Tel: 646 794 0654
E: adam.sills@awac.com

ALLIED WORLD ASSURANCE COMPANY

SALLOP
Insurance Brokerage ▪ Risk Mitigation ▪ Special Risks

www.awac.com