BSR
PO Box 768 · Hendersonville, TN 37075
(T) 800-768-7475 · (F) 615-264-3980
www.bsrins.com

DATA PRIVACY & SECURITY

DataBreach℠ for Healthcare Facilities and Providers

MARKEL®

www.markelcorp.com

Classes We Consider

- Blood Center
- Medical Screening Service
- Clinics
- Rural Acute Care Hospital
- Laboratory
- Physician Practices
- Medical Billing
- Telemedicine Practice
- Electronic Medical Records

Assess the Risk Reality

- Does the company use portable "jump" or "thumb" drives to transport files and information?
- Is every business laptop encrypted?
- Are backup tapes used and carried off-site?
- Does the emerging threat of healthcare benefits fraud pose a risk to the business?
- Does the business owner realize that, although employees' access to sensitive data may be monitored, the way they use that data is impossible to control?
- Has anyone in the business ever been asked to give out their password over the phone to diagnose a technical problem?
- Does the business use the services of third parties for data storage, IT systems support or management, collections, processing medical claims, or tele-radiology?

What Does DataBreach℠ Offer?*

- Regulatory defense with no sub-limit
- Coverage includes liabilities arising from the theft or loss of paper records
- Vicarious liability for data entrusted to Business Associates or other third parties (by endorsement)
- Liability from identity theft, including medical identity theft
- Media coverage for information on the business website, including whitepapers and content
- Recovery costs and extra expenses due to unauthorized access to data systems
- Punitive damages (when insurable by law)
- Claims-made form
- Claim team dedicated to medical and allied healthcare professionals
- Coverage through an insurance partner with a stable history in the healthcare line
- Limits up to $5 million
- Supplementary payments coverage in addition to the limits, and not subject to the deductible, is available for compliance with security breach notice laws, voluntary credit monitoring, and public relations expenses

[1] Compiled from data at www.etiolated.org
[2] From www.ihealthbeat.org; July 2, 2008
[3] *Reno Gazette-Journal* online at www.rgi.com; July 24, 2008
[4] *Arkansas Democrat Gazette* online at www.nwanews.com; July 2, 2008
[5] WSBT 2 News; online at www.wsbt.com; February 7, 2008
[6] *U.S. News & World Report* online at www.usnews.com; February 29, 2008
[7] The Council of Insurance Agents & Brokers online publication at www.ciab.com; August 20, 2008; and *Computerworld Security*; online at www.computerworld.com; September 7, 2007

*Coverage available through Markel regional offices: Markel Midwest, Markel Mid South, Markel Northeast, Markel Southeast and Markel West. For information refer to www.markelcorp.com. For complete terms and conditions, refer to the policy itself. Coverage is subject to conditions and exclusions in the policy.

4/28/09

MARKEL®

www.markelcorp.com

DATA PRIVACY & SECURITY

DataBreach℠ for Healthcare Facilities and Providers

Since the introduction of HIPAA regulations in 1999, increased attention has been paid to the care and keeping of medical records. Security for all data, both paper and electronic, has been an evolving issue that becomes more complex as we move further into a paperless age. Storage and processing of Protected Health Information, credit/debit card and electronic check payments, Social Security numbers, employee data, and health insurance claim submissions all present opportunities for data breaches.

Despite developing safe recordkeeping practices, adherance to these practices and precautions does not guarantee avoidance of incidents resulting from human behavior. In fact, reports indicate that 6,093,661 medical records were compromised between September 1, 2006 and September 1, 2008.[1] What's worse, general liability policies do not cover most of these situations.

In the News

- Backup tapes from the University of Utah were stolen from a car belonging to an independent storage company, but were eventually recovered. The tapes contained billing data, Social Security numbers, and medical procedure codes dating back to 1992 for 1.5 million patients. Notification expenses cost the hospital roughly $500,000 and lawsuits have been filed by patients. The expense of one year of free credit report monitoring for those affected was also incurred.[2]
- An unauthorized person may have gained access to the Saint Mary's Regional Medical Center (Reno, NV) database of 128,000 patient records, which included limited health information and Social Security numbers. The hospital worked with Equifax to mitigate patient issues.[3]
- An emergency department employee of Baptist Health Medical Center in North Little Rock, Arkansas was arrested for financial identity fraud. The employee and a friend may have used personal data from 1,800 patients for financial gain. This occurred despite the health system's continual audits of staff access to information.[4]
- An employee of Memorial Hospital in South Bend, Indiana lost a laptop while traveling. The computer contained names, addresses, birth dates, ID numbers and Social Security numbers for about 4,300 full- and part-time employees and retirees. The hospital offered one year of free credit report monitoring to staff and alums to mitigate further issues.[5]
- A front desk clerk for the Cleveland Clinic in Weston, Florida stole the names, addresses, Social Security numbers, and Medicare numbers of more than 1,100 patients. She sold them to her cousin, who then filed false Medicare claims in excess of $2.8 million.[6]

How Great is the Risk?

Seattle-based Providence Home and Community Services and Providence Hospice and Home Care had several instances of lost backup tapes, optical disks, and laptops. These situations resulted in the first fine ever levied by the Department of Health and Human Services for HIPAA violations, and a $95,000 settlement for direct financial losses stemming from thefts of information. Per state law, 386,000 patients had to be notified of the incident. Providence also offered free credit report monitoring services for a year to affected individuals. One estimate places the cost of these two items at over a million dollars.[7]

Receive cash for breach mitigation expenses, public relations, client notification, and voluntary credit monitoring with DataBreach℠ coverage.*

DataBreach℠ coverage, while it will not pay for fines, does offer coverage for defense of regulatory actions which is not subject to a sub-limit.*