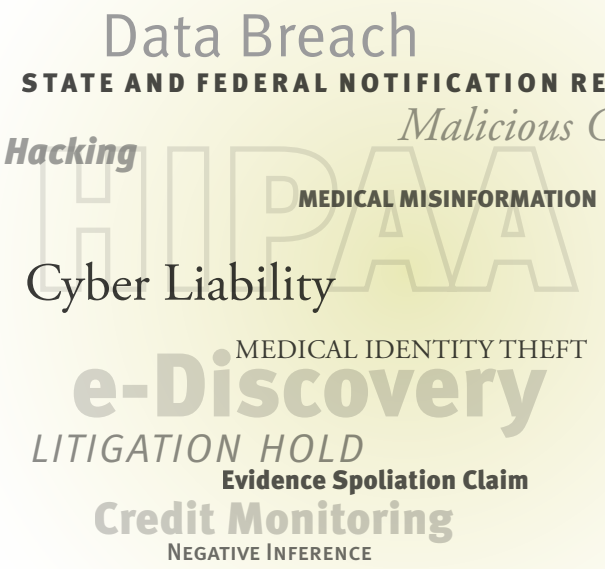
INSURING MEDICINE AGAINST NEW TECHNOLOGICAL RISKS

Cyber Liability and e-Defense Coverage



...and you thought it was safe to go in to work today!

Welcome to the new world of medical risk. In today's ever changing medical practice environment, your clients are being asked to do more with less. The Federal Government is pushing the health care world into the electronic universe. The economic stimulus package has provisions for electronic medical record systems; the question is no longer if your clients will go electronic—it's when. If any of the terms on the left seem unfamiliar to you or your clients, we can help.

ProAssurance is the first professional liability company to provide combination Cyber Liability and e-Discovery Expense Coverage. This coverage has been designed specifically for the health care industry and reflects the experience and expertise of ProAssurance companies—one of the largest professional liability coverage providers to the medical community.

Wonder about the need for such coverage for your clients? Read on for numerous examples that have occurred over the last three years.

(continued on the reverse side)

PROASSURANCE®
Treated Fairly

ProAssurance Specialty Insurance Company, Inc.

email: esl@proassurance.com • ProAssurance.com
Call: 800.282-6242, extension 4762

INSURING MEDICINE AGAINST NEW TECHNOLOGICAL RISKS

Cyber Liability and e-Defense Coverage

"Do my clients really need this?"

EXAMPLES TO CONSIDER:

- A laptop containing the health care information of about 100,000 patients of Baylor Health Care Systems in Texas was stolen from the car of an employee—who was subsequently fired for breaking company protocol. Baylor is offering free credit-monitoring services to the victims whose Social Security numbers were on the laptop.

  SOURCE: Jason Roberson, "Baylor Health Care says laptop with patient data stolen," *The Dallas Morning News*, November 4, 2008.

- A laptop containing sensitive data on 45,000 patients, employees, and physicians from Sutter Lakeside Hospital in Lake County, California, was stolen from a contractor's home. "We work in an environment where protecting individuals' information is absolutely as important as providing quality service and care. Storing this type of information on a laptop hard drive is at variance with our organization's strict policies" says hospital CEO Kelly Mather.

  SOURCE: Elizabeth Wilson, "Stolen laptop holds private information," *Lake County Record-Bee*, December 10, 2007.

- "Johns Hopkins officials have hired an independent forensic scientist to investigate whether patient information on a stolen desktop computer was accessed. The computer, which contained patient information in a tumor registry database, was stolen from the East Baltimore Campus of Johns Hopkins Hospital July 15 [2007]. Hopkins officials sent out letters to impacted patients [the last week in August]."

  Source: Sue Schultz, "Stolen hospital computer returned; Hopkins hires investigator to probe data breach," *Baltimore Business Journal*, September 4, 2007.

- Patient records were available by web search during a four-week period after Sky Lakes Medical Center in Oregon shut down its online bill-payment system, and a third-party, Verus, Inc., transferred the data from one server to another to perform maintenance. The hospital sent letters to 30,000 patients warning them of the problem.

  Source: "Online bill pay at Sky Lakes shut down," *Klamath Falls Herald and News*, August 15, 2007.

- The personal information of approximately 128,000 clients and patients of St. Mary's Regional Medical Center in Reno, Nevada was potentially compromised when a database was illegally accessed. The hospital is offering one year of free credit monitoring to those patients whose Social Security numbers were stored in the database.

  Source: Dan Kaplan, "St. Mary's warns of possible data leak," *Reno Gazette-Journal*, July 24, 2008.

- The names, addresses, and Social Security numbers of about 51,000 patients of St. Vincent Indianapolis Hospital were made available on the web because of a security lapse by a third-party vendor.

  Source: Daniel Lee, "Data lapse involved 51,000, St. Vincent says," *The Indianapolis Star*, July 25, 2007.

- Atlanta's Grady Memorial Hospital recently found out that records on 45 of its patients ended up on an unsecured, public website and remained available for a few weeks. The data included doctors' notes, medical conditions, diagnoses, documentation of medical procedures, and, possibly, names and ages of patients, the hospital said.

  Source: Craig Schneider, "Human error to blame for Grady data breach," *The Atlanta Journal-Constitution*, September 23, 2008.

- "Akron—Overseas hackers have apparently accessed two computers at Children's Hospital, one containing private patient data, the other billing and bank information. The hospital is preparing to send out more than 200,000 letters informing patients of the breach. It's also given the F.B.I. information for the investigation. The hackers apparently were from Germany and used computer loops through France, Turkey, and Canada, eventually landing data from Akron. 'It's absolutely terrifying in this day and age where information is power,' says patient Jennifer Ferrick. 'Privacy is of the utmost importance in the medical field.'"

  Source: Vic Gideon, "Computer breach at Children's Hospital," WKYC-TV, October 26, 2006.

- "Doctors' offices, clinics and hospitals are a fruitful hunting ground for identity thieves, who are using increasingly sophisticated methods to steal patient information, lawyers and privacy experts say. Recent disclosures that hospital workers snooped into the medical files of Maria Shriver, Britney Spears and George Clooney highlight the vulnerability of patients to the merely curious and the criminal. Legal experts say lawbreakers use medical information to get credit card numbers, drain bank accounts or falsely bill Medicare and other insurers. Pam Dixon, executive director of the World Privacy Forum, an advocacy group, says 'sophisticated crime rings' often can make more money by stealing medical identities than by going after individuals' bank accounts or credit cards. 'If you steal someone's medical identity, then multiply that by 100 or 1,000 other thefts and do fake billings, you can make hundreds of thousands, if not millions, of dollars,' Dixon says. In Florida last year, a front-desk coordinator at the Cleveland Clinic was convicted of identity theft, computer fraud and other charges after downloading patient information and selling it to a cousin, who submitted more than $2.5 million in phony bills to Medicare. In April, a former New York-Presbyterian Hospital employee was arrested for participating in an identity theft scheme in which he allegedly accessed nearly 50,000 patient records over two years."

  Source: Julie Appleby, "Identity thieves prey on patients' medical records," *USA TODAY*, May 7, 2008.

Taking proactive risk management steps and having the right insurance protection is the solution...

Please contact **ProAssurance Specialty Insurance Company, Inc.** to find out how we can help you solidify your client relationships and expand your business opportunities.

As a surplus lines insurer, ProAssurance Specialty Insurance Company, Inc. does not participate in the state guaranty funds.

PROASSURANCE®
Treated Fairly

email: esl@proassurance.com • ProAssurance.com
Call: 800.282-6242, extension 4762