

## HEALTHCARE INDUSTRY



### PROFILE OF CLIMATE

Over the past 5 years, numerous legislation regarding use and protection of proprietary information by corporations, and how it is secured and transported by healthcare companies, has created unprecedented exposure for the healthcare industry. These laws include HIPAA, and Calif. Security Breach Act 1386 revised in 2008 to CA1798, which not only enhances the healthcare standard of care required, but also carries civil liability if notification rules aren't followed. A breach of secure information can cost on average \$202 per record with an average claim of \$6.6 million (Ponemon Institute Study 2009). These costs are escalated should they include any HIPAA investigation or fines. The domino effect of prolific costs can virtually put a healthcare firm out of business, not for arbitrary technology E&O damage, but by legislative mandated costs. Lack of standards of care for your technology infrastructure, background checks, software update non conformity, lack of sophisticated encryption processes, wireless networks, loose laptop tracking, to name a few, can all lead to enormous exposures for your healthcare firm. These breaches of secure healthcare information have quickly escalated into class action lawsuits and HIPAA fines in excess of \$100,000.

### COVERAGE OVERVIEW

Claims made policies with Premiums ranging from \$1k to over \$100k for more complex coverage typically requiring worldwide coverage with limits ranging from \$250k to \$25million and deductibles from \$1k upward to \$100k.

### COVERAGE AVAILABLE

Note that many ISO exclusions exist for electronic information including explicit exclusions on almost all CGL and GL coverage forms.

**Cyber coverage** for 1st and 3rd party malicious code

**Secure Data** coverage for breaches of CA 1798, HIPAA, and all states secure data laws including Red Flag Rules, PCI Rules etc

**Business Interruption** for loss of revenue during security breach crisis

**Crisis Management** reimbursement to cover costs of team to help remediate and control the incident including PR spin and Media costs

**Intellectual Property** for perils like trademark, copywrite and patent infringement

**Errors and Omissions** coverage for malfeasance of the technology implementation team and their

subcontractors associated with any professional technology service for a fee.

**Personal Injury** to cover defamation, invasion of privacy or related perils

**Call Center Support** to handle costs associated with massive Q&A load from breached clients

**Legislative Compliancy** Coverage for certain fines and costs associated with investigations and penalties associated with HIPAA, GLB etc

**Cyber Extortion** perils associated with outside demands for money to not release info or threatening to take down the technology infrastructure.

**BI** coverage for bodily injury

### CLASSES OF HEALTHCARE COMPANIES

Doctors, dentist, or any medical providers office, All Healthcare providers such as hospitals, surgery centers, home health care, pharmacies, Med spas, MRI centers, Radiologists, Labs, Medical records, storage and transcription, Third party administrators, health benefits agents, anyone handling healthcare information etc.

## QUESTIONS ABOUT YOUR INSURED'S

- Any secure data breaches or incidents in last 5 years?
- Do you use independent contractors or subcontractors for internal technology?
- Do you require E&O coverage for your contractors?
- Do you have any compliance certificates (PCI, HIPAA, etc)?
- Do you work with outsource companies that collect and keep any proprietary info such as (SS#, Credit card info, medical info, account numbers, maiden names, pets names etc)?
- Do you as standard procedure encrypt data on all laptops, backups, emails etc.?
- Do you use and or implement any wireless networks?
- Do you have any corporate policy or procedures for identity theft or secure data breaches?
- Do you have any patents, copywrite, trademarks or intellectual property?
- Do you have a transactional website in any way?
- How often do they change passwords for their systems and do they contain a combination of letters and numbers over 8 characters?
- Do you do business in multiple states and or worldwide?
- Are you Red Flag Rule Compliant?

**A breach of  
secure information  
can cost on average  
\$202 per record  
with an average claim of  
\$6.6 million**

## CLAIMS EXAMPLES

### **Claim 1 - Providence Class Action Lawsuit and HIPAA Fines**

Providence Home Services of Portland Oregon in 2006 had 365,000 records stolen on laptops and backup tapes that were not encrypted and contained patient information including financial information on some patient records. Oregon attorney general in 2008 forced secure data settlement to include monitoring and reimbursement of personal losses and severe measures to update and encrypt all future information and submit to random inspection measures to be monitored by Health and Human Services Dept including a \$100,000 fine for lack of HIPAA standards of care. The class action is still open and ongoing. Costs already over \$1.2m

### **Claim 2 - Cyber Claim and Secure Data**

A woman purchased a used computer from a pharmacy. The computer still contained the prescription records, including names, addresses, social security numbers and medication lists of pharmacy customers.

**Consequence** - The cost of notifying affected parties per state law totaled nearly \$110,000. Two lawsuits have been filed: one alleges damages in excess of \$200,000 from a party who claims she lost her job as a result of the disclosure; the second alleges that the plaintiff's identity was stolen, and that costs of correction and emotional distress will exceed \$100,000. A HIPAA investigation is also underway and will further add to the costs of the claim, not to mention possible HIPAA fines.