

Enterprise Privacy Protection Insurance

Designed for the Healthcare Sector

Liability insurance to cover you following a breach of privacy or computer network security, including crisis management and customer notification expense

The privacy and security risk environment for healthcare organizations continues to be a progressively more important concern and has become a priority on most boardrooms agenda. As personal sensitive health information becomes increasingly available in electronic form as new technologies are integrated in the day-to-day operations, so has the security of protection of such information. Healthcare organizations are subject to compliance with very stringent regulations, such as the Health Insurance Portability and Accountability Act (HIPAA). Traditional property & casualty insurance policies are inadequate and typically do not address these merging new risks that could result in severe financial consequences.

JLT's exclusive Enterprise Privacy Protection policy has been designed to specifically fill these insurance cover gaps. The policy is underwritten by Lloyd's of London and was first introduced in March 2005

Main Insuring Clauses Enterprise Privacy Protection

Section	Sum Insured
<p>A. Third Party Privacy Liability Sums the insured is legally obligated to pay as damages and claims expenses as a result of a privacy breach or breach of privacy regulations. The definition includes common law breach of confidence, HIPAA, Gramm-Leach-Bliley Act, privacy protection laws and privacy provisions of the Federal Fair Credit Reporting Act.</p>	US\$ Policy limit Any one claim and in all during the policy period.
<p>B. Employee Privacy Liability Same as coverage A but the plaintiff is an employee (excluding claims arising out of employment practices liability or ERISA violations).</p>	US\$ Policy limit Any one claim and in all during the policy period.
<p>C. Privacy Regulatory Defence and Penalties Defense of a regulatory action, complaint, investigation including indemnification for a penalty, civil fines, or sanction imposed by a federal, state or regulatory body, as a direct result of a privacy breach or breach of privacy regulations as defined.</p>	Up to US\$2,000,000 Any one claim and in the annual aggregate limit of insurance. Subject to pre-agreed coinsurance participation.
<p>D. Crisis Management and Customer Notification Expenses Cover for:</p> <ul style="list-style-type: none"> • public relations services to protect brand/image related to a claim, penalty, civil fines or sanction covered under the other insuring clauses • notification expenses to warn customers or patients of security breaches as required by many state laws. 	US\$1,000,000 Any one occurrence without application of any policy
<p>E. Security Liability Sums the insured is legally obligated to pay as damages and claims expenses arising out of computer attacks caused by failures of security including theft of client information, identity theft, negligent transmission of computer viruses and denial of service liability. Broad coverage is provided to address insiders as perpetrators and provide coverage for "failure to warn" obligations created by state laws, such as the California Data Protection Act (SB1386).</p> <ul style="list-style-type: none"> • Affirmative coverage for "phishing" and "pharming" i.e. false communications designed to obtain personal information. • Security coverage extends to the protection and confidentiality of all customer records or information, not just that contained in computer systems. • HIPAA and federal, state privacy laws. • Contractual coverage for breach of the insured's privacy statement. • Expanded definition of "privacy breach" and "privacy regulations". Basically follows what a regulator deems to be privacy rather than a more limited insurer definition. 	US\$ Policy limit Any one occurrence and in all during the policy period.

Key cover features of Privacy and security risk background

Why this is a boardroom issue

Cost and efficiency objectives and technology advances have encouraged companies in the healthcare sector to increase IT investment and usage. Today, innumerable transactions and patient-related functions are performed using public and private networks, including new wireless applications. Whilst this has undoubtedly delivered many benefits it has also created additional and more complex risks, potentially increasing the privacy and security risk exposure. Publicity and business risks are extensive, particularly for entities subject to the accountability and internal control requirements of the Sarbanes-Oxley Act. The Symantec Internet Security Threat Report (April 2008) found

that the healthcare industry sector ranked third in data breaches that could lead to identity theft. And perpetrators of security data breaches are not just external persons or gangs, they also emanate from employees or independent contractors. There are many reasons for a computer attack, ranging from extortion to identity theft. This frequently involves unauthorised access or use of computer networks, use of spyware and malicious code "malware" and denial of service attacks. It can leave an organization facing potential liability and own damage costs, as well as the effect it has on their reputation.

Attacks on major educational Institutions aimed at accessing student and patient information, including pharmacy and hospital databases, have been widely reported. In one incident there was a threat to post the records on the Internet (www.healthprivacy.org). The first HIPAA privacy conviction in 2004 involved a former employee of a cancer treatment centre who used patient information to obtain credit cards and buy merchandise (www.usdoj.gov). All healthcare related entities (including health plans, healthcare clearing houses, healthcare providers, hospitals) are subject to HIPAA Privacy Rules that were put in to mandatory compliance as of April 1, 2005. These regulations provide patients with rights to control their protected healthcare information (PHI), limit use and disclosure of such information and protect the integrity and confidentiality of electronic PHI. These rules also affect persons or entities that perform functions for and have contracts with "covered entities", for example healthcare related claim processors, professional services and technology providers. Violation of HIPAA rules can result in considerable legal defense associated with a regulatory investigation and civil fines. Although there is no private course of action under HIPAA, the requirements potentially create a standard and duty of care that can bolster a civil claim and compliance creates documents that might be used as evidence.

Additionally, over 40 states have enacted notification laws that require entities, including healthcare industry, to notify individuals loss or theft of data from security breach. These notification costs can range into the millions of dollars for these organizations who experience a security breach.

Technology Liability and Cyber Risk Experts

JLT has a specialist Technology Liability and Cyber Risks team advising many leading corporations around the world and providing specialist access to the London insurance market. JLT is part of the Jardine Lloyd Thompson Group of Companies, a leading risk management adviser, insurance and reinsurance broker and major provider of employee benefit administration services and related consultancy advice. Jardine Lloyd Thompson Group plc is quoted on the London Stock Exchange and is the largest European-headquartered company providing these services and is one of the largest firms of its type in the world.

Other Technology and Cyber Risk Products

JLT has developed a range of Technology and Cyber Risk products providing third party liability, first loss property and business interruption coverage.





Why Purchase Enterprise Privacy Protection?

Traditional insurance policies do not usually provide adequate protection. Crime policies generally do not cover stealing data or consequential damages. Professional Liability and Medical Malpractice policies may not provide privacy risk protection or coverage for intentional acts of employees. Generic cyber liability products may not address the scope of coverage needed for privacy and security risks following the HIPAA Rules and typically exclude coverage for civil fines, penalties from regulatory complaints.

To find out more contact:

Simon Milner

+44 (0) 20 7558 3647
simon_milner@jltgroup.com

Warren Hattwich

+44 (0) 20 7558 3457
warren_hattwich@jltgroup.com

Or visit our web site

<http://www.jltgroup.com/it-risk-assessment>

This document is for information only and in no way overrides or forms part of any Enterprise Privacy Protection policy. It does not constitute an offer of insurance of any kind, nor should it be relied upon as a description of precise coverage which may be available under any Enterprise Privacy Protection policy. If you would like to see a full copy of the standard policy wording please contact simon_milner@jltgroup.com.

JLT Specialty Limited

6 Crutched Friars
London EC3N 2PH
Tel +44 (0)20 7528 4000
Fax +44 (0)20 7528 4500
www.jltgroup.com

Lloyd's Broker. Authorised and Regulated by the Financial Services Authority. A member of the Jardine Lloyd Thompson Group. Registered Office: 6 Crutched Friars, London EC3N 2PH. Registered in England No. 01536540. VAT No. 244 2321 96.

© January 2011 262916