PRS - CareNet Security: APPLICATION FORM

Please answer all questions on this form. Before any question is answered please read carefully the declaration at the end of the application form which you are required to sign.

1) Applicant(s): _____

2) Address: _____

3) Nature of Business: Long Term Care facility

4) No. of Employees: ____

5) Revenues: This Application is for risks with total revenues no greater than USD50,000,000:

Total revenues i) for the current financial year: USD _____

ii) projected for the next financial year: USD _____

6) Website home page; _____

Does site have a Privacy Statement? ☐ Yes ☐ No

7) Does Applicant have established procedures for editing or removing from your website libelous or content that infringes the Intellectual Property rights of others (copyright, trademark, trade name, trade secrets etc.)?: ☐ Yes ☐ No

8) Does Applicant have a) an email & internet usage policy that has been shared with all staff, b) firewall system in place, c) mandatory individual unique non-trivial ID and passwords with periodic password changes, and d) all PCs and servers protected with up-to-date anti-virus software ? ☐ Yes ☐ No

9) Please indicate the total number of PII* records stored on your network: _____

* PII being personally identifiable information including but not limited to Personal Medical Information, Social Security Information , Debit or Credit Payment Card Details, and Financial Information)

10) Does Applicant currently have and Privacy or similar insurance in force: ☐ Yes ☐ No

If Yes then please provide Retroactive date: _____.
Please also provide details below and attach evidence of expiring coverage (e.g. Declaration page) hereto.

11) Has Applicant

i) ever sustained a significant system intrusion, tampering, virus or malicious code attack, loss of data, hacking incident, data theft or similar incident? ☐ Yes ☐ No

ii) in past 3 years had anyone allege their personal information was compromised, or have you notified customers that their information was or may have been compromised? ☐ Yes ☐ No

iii) sustained any unscheduled network outage or interruption in the past 24 months? ☐ Yes ☐ No

iv) in past 5 years experienced any claims or are you aware of any circumstances that could give rise to a claim that may have been covered by this policy? ☐ Yes ☐ No

If Yes to any of the above then please provide details (continue on separate sheet if required)

Declaration: I HEREBY DECLARE THAT I AM AUTHORIZED TO COMPLETE THIS APPLICATION ON BEHALF OF THE APPLICANT AND THAT AFTER DUE INQUIRY, TO THE BEST OF MY KNOWLEDGE AND BELIEF, THE STATEMENTS ANI PARTICULARS IN THIS APPLICATION ARE TRUE AND COMPLETE AND NO MATERIAL FACTS HAVE BEEN MISSTATEI SUPPRESSED, OR OMITTED

Signed:* _____ Name*: _____

Position:* _____ Date*: _____

*the signatory should be an owner director or senior officer of, or a partner in, the Applicant

PRS - CareNet Security: HIGHLIGHT SHEET

CareNet Security Wording Coverage Highlights

- **Privacy** including:
  - Notification costs
  - Credit reporting monitoring
  - Crisis management costs
  - Regulatory violations (including HIPAA), defense costs & fines
  - Forensic costs
  - Employee privacy
- **Cyber Extortion**
- **Network Business Interruption & Loss of Data**
- **Personal and Advertising Injury**
- **Media Liability**
- **Intellectual Property Liability** including:
  - Infringement of copyright, trademark, service mark, or trade name
  - Domain name,
  - Trade dress, title or slogan
- **Trade Secret Disclusure, Plagiarism, Piracy or Misappropriation of Ideas**

Minimum Premium: **$1,200**

Minimum Deductible: **$1,000**

Available Limits: **$2,000,000**
Excess Limits are available on request

CareNet Security is Underwritten by Syndicates at Lloyd's of London and in conjunction with Safeonline LLP

Access to Class leading Vendors/Experts

- **Risk Management provided in conjunction with Safeonline LLP and IdentityTheft 911**
  - see attached **RISK MANAGEMENT** sheet
- **Theodore J. Kobus III of Baker Hostetler, acting in role of Defence Counsel**

Examples of Large Data Risks for Small Businesses

Small and mid-size businesses face growing data breach threats and costs. Privacy Rights Clearinghouse reports over half a billion records exposed since 2005. Featured expert, Brian McGinley, Identity Theft 911 SVP, Data Risk Management, provides proven strategies to help businesses protect information assets, mitigate risks and recover from breach incidents.

Q. Don't breaches just hit huge companies, like Sony and Epsilon?

McGinley: No, those are just front-page news. Breaches strike businesses of all sizes. In fact, the Verizon 2011 Data Breach Investigations Report shows that small to mid-tier organizations have become hackers' main targets lately. Attacks can be costly, causing serious financial stress.

Q. Is cyber risk the only worry?

McGinley: Absolutely not. Also consider: a lost laptop with no password, a missing and unencrypted back-up drive or smartphone, and paper files that aren't properly shredded. Also watch for careless employees and vendors; prying eyes watching computer screens at the office or in public areas where employees may be working; sensitive data left unattended at copy, fax machines and in-boxes; and files stored in unlocked cabinets. New vulnerabilities and exposures are emerging daily.

Q. What safeguards can be taken?

McGinley: When it comes to protecting information assets, the best defense is a great offense. Privacy protection can be a competitive advantage, too. Start by taking care of the basics: keep sensitive data out of unauthorized reach; restrict access to data; lock it up; only keep information that's necessary; put security systems in place; and screen employees and visitors. Limit the use of portable technology; avoid unsecured wireless networks; ensure network security; install antivirus, anti-spyware and firewalls; always use password protection and encryption; and regularly review data practices.

Q. How can small businesses be prepared without breaking the bank?

McGinley: You don't have to be a Fortune 500 company to follow a data security approach called Privacy by Design (PbD). Simply put, PbD is a logical way to assess your operation. It starts by taking a hard look at your company's data—how it's received, used, stored, retrieved and disposed. The key is to overlay each process in the data stream with the best privacy and security practices. At each step of the data lifecycle, a business owner needs to ask, "How can I best protect this data?". Businesses also must have a formal incident response plan in place. This defines a step-by-step breach how-to plan, contact information for your security team, your security policies and practices a continuity plan for business and disaster recovery, and employee/staff privacy policy.

Q. What could a breach cost?

McGinley: Potentially tens of thousands of dollars or more, since organizations have to pay for the costs to provide notice, monitoring services and services to help resolve identity theft to all potential victims. There may also be secondary liability costs and defense expenses associated with actions by vendors, credit card payment processors, customers and regulators. Also consider the cost of clean up, reputation compromise and any lost business.

Q. Won't the business' commercial policy cover these costs?

McGinley: Very few business policies provide the combination of services; support and insurance that the experts agree you need to cover the emerging risks. Be sure to ask your insurance company if you have such coverage in place.

Better still talk to PRS about CareNet Security

PRS - CareNet Security: RISK MANAGEMENT

What is a Data Breach ?

A loss, theft, accidental release or accidental publication of Personally Identifiable Information (PII) or Protected Health Information (PHI) including Social Security number, Bank account, credit or debit number, Driver's license number, PIN numbers, Medical diagnosis, patient history/medications, and other private information defined by state or federal law

Who needs this coverage?

Virtually no business is immune from this potential risk. All businesses that handle or store any private business, customer or employee data is at risk for a data breach and could benefit from this coverage. The possibility is esp high for firms that routinely deal with credit cards, patient medical records, Social Security numbers and other sensitive PII or PHI.

How can a data breach occur?

- Unauthorized access (such as by former employees, vendors or hackers)
- Stolen or lost paper fi les, or shipped documents failing to arrive at proper destination
- Mailing, faxing or emailing documents with one person's PII to the wrong person
- Computer system hacked by virus, Trojan horse or improper security
- Stolen/lost laptop, computer disks, USB flash drives, portable hard drives or back-up tapes
- Employee error or oversight

Are you prepared for a Data Breach ?

Professional Risk Solutions, in conjunction with certain Underwriters at Lloyd's and Identity Theft 911, are pleased to offer a Data Breach Privacy and Insurance product to help protect your good name with :

- Access to breach preparation and crisis management assistance to confidently assess the situation
- Trusted resources to confidently manage the crisis and control the damage to safeguard your business reputation, help prevent sanctions and fi nes and avoid civil litigation.
- Delivery of timely notification to preserve customer and employee goodwill, and access to personalized fraud specialist assistance if any become victims of identity theft or fraud as a result of the breach.
- Access to resources through a secure breach preparedness Website

What makes our Data Breach offering unique?

PRS CareNet Security includes proactive & post-breach services to help minimize occurrence of a data breach and expert assistance if one occurs.

Resources available to you with your PRS CareNet Security policy:

You will have access to a proprietary breach preparedness website, powered by Identity Theft 911 providing:

- Tips & resources to help you minimize risk and info on how to safeguard PII/PHI for customers, patients and employees
- Details on how to create a data breach incident responseplan including drafting breach notification letters
- Guidance on what needs to be done if a breach occurs
- Legal requirements by state

IDentityTheft 911
Protecting identities. Enhancing reputations.

Claims Handling Process

1. Policyholder contacts claims representative

- Please call at the first sign that a breach has occurred, or if you suspect a breach or have any breach related question or concern.
- Claims representative will:
  - o Verify eligibility
  - o Record contact information
  - o Tell you that an IDT911 breach consultant will be contacting policyholder within one business day

2. Underwriters Claims Representative Contacts IDT911

- Provides contact information for both you and claims representative, including:
  - o Company name
  - o Contact name
  - o Telephone number
- Indicates if he/she wants to be involved in breach handling and if policyholder has breach reimbursement policy.

3. IDT911 contacts and works with you to provide:

- Answers to any breach-related questions of concerns
- Evaluation of the severity of a breach
- Assistance with crisis management
- Guidance with best practices regarding handling a breach, incl. regulatory and liability aspects of responding to a breach
- All necessary support document templates
- Help with all notifications to affected parties, regulators, credit bureaus, state attorney general offices and departments of consumer affairs
- Support with media interface and a press release, if requested
- Assistance in offering optional monitoring products