ASPEN AMERICAN INSURANCE COMPANY

BROKERING AGENT'S REGISTER No. _____
[Florida Applicant's Only]

PROFESSIONAL PROTECTOR PLAN FOR DENTISTS | PPP

The Professional Protector Plan®

Supplemental Application for Cyber Liability & Data Breach Coverage - Florida

ASPEN AMERICAN INSURANCE COMPANY
(A stock insurance company)
Administrative Offices: 590 Madison Avenue, 7th Floor, New York, NY 10022

THE POLICY YOU ARE APPLYING FOR MAY PROVIDE CLAIMS MADE COVERAGE, WHICH APPLIES ONLY TO CLAIMS FIRST MADE DURING THE POLICY PERIOD, OR DURING AN APPLICABLE EXTENDED REPORTING PERIOD. THE LIMIT OF LIABILITY TO PAY DAMAGES OR SETTLEMENTS WILL BE REDUCED AND MAY BE EXHAUSTED, BY CLAIM EXPENSES, AND CLAIMS EXPENSES WILL BE APPLIED AGAINST THE DEDUCTIBLE, UNLESS OTHERWISE PROVIDED BY THE POLICY. IN NO EVENT WILL THE INSURER BE LIABLE FOR CLAIMS EXPENSE OR THE AMOUNT OF ANY JUDGMENT OR SETTLEMENT IN EXCESS OF THE APPLICABLE LIMIT OF LIABILITY.

THIS APPLICATION IS NEITHER AN OFFERING NOR A BINDER OF COVERAGE. ALSO, YOUR COMPLETION OF THIS APPLICATION DOES NOT OBLIGATE THE COMPANY TO OFFER COVERAGE TO YOU.

Applicant's General Information

1) Applicants name (name of firm or practice as it appears on your professional liability policy. _____
2) What is your annual Gross Revenue? Current year $ _____. Next Year $_____
3) For how many patients in total (practice –wide) do you have records in custody? _____
4) What's the maximum number of patients for whom you store records in any one location? _____
   (For example, on one laptop? Disk? Server? In off-site storage?)
5) If you currently carry cyber or information risk coverage, what's the inception date of your first such policy?
6) **Other than patient data**, please describe other sensitive information in your care (e.g. vendor data, other's trade secret or proprietary info etc. .) _____
7) Please identify the services that you outsource to others by completing the entries in the table below.

Type of outsourced service	Primary Vendor	Other Vendors used
Hosting		
Financial services and payments		
Billing service		
Back-up & data recovery		
Shredding & data destruction		
Electronic medical record conversion & management		
Records management or archive service		
Internet Service Provider		
Please identify any other services & vendors		

Loss History

8. After inquiry of all owners, partners, officers and professionals of the practice and the practice affiliates, within the last five years:

   a. have any past or present personnel received any complaints, claims or been subject to litigation or regulatory action or inquiries involving matters of, or similar to: privacy injury, identity theft, Denial of Service attacks, computer virus infections, theft of others' information, damage to your network or others networks, others' inability to rely on your

network, or extortion demands involving your network or information in your care? ☐ Yes ☐ No

b. are any of the owners, partners, officers and professionals of the practice and the practice affiliates aware of, any prior incident, circumstance, or litigation that could reasonably give rise to a claim under this Policy ? ☐ Yes ☐ No

c. have you sustained a privacy breach, loss or unauthorized disclosure of private or sensitive information? ☐ Yes ☐ No

If Yes, how many in the past 5 years? _____

If "yes" to any part of question 8. above, please use a separate attachment to describe the date, location, nature, circumstance, loss and any subsequent preventive measures taken by your firm in association with the incident.

It is agreed by all concerned that if any of the individuals or organizations proposed for coverage under this Policy is responsible for or has knowledge of any incident, circumstance, event or litigation which could reasonably give rise to a claim, whether or not described above, any claim subsequently emanating there from shall be excluded from coverage.

Risk Control Self Assessment

Please circle yes (Y) or No (N) or Not Applicable (NA) for each question.

1. Do you enforce a company policy governing security, privacy and acceptable use of company property that must be followed by anyone who accesses your network or sensitive information in your care? **Y / N**
2. Do you prominently disclose your privacy policy and always honor it? **Y / N**
3. Do you implement virus controls and filtering on all systems? **Y / N**
4. Do you check for security patches to your systems at least weekly and implement them within 30 days? **Y / N**
5. Do you replace factory default settings to ensure your information security systems are securely configured? **Y / N**
6. Do you re-assess your exposure to information security and privacy threats at least yearly, and enhance your risk controls in response to changes? **Y / N**
7. Do you authenticate and encrypt all remote access to your network and require all such access to be from systems at least as secure as your own? Check NA **ONLY** if you do not allow remote access to your systems. **Y / N / NA**
8. Do you physically and electronically limit access to sensitive information on a need to know basis and revoke access privileges upon a reduction in an individual's need to know? **Y / N**
9. Do you enforce a "clean desk" policy in which sensitive information must not be accessible or visible when left unattended? **Y / N**
10. Do you enforce a "clear screen" policy that includes clearing computer screens and requiring user logon and password authentication to re-access the device after a period of inactivity? **Y / N**
11. Do you outsource your information security management to a qualified firm specializing in security or have staff responsible for and trained in information security? **Y / N**
12. Whenever you entrust sensitive information to 3rd parties do you (you should check NA **ONLY** if you never entrust sensitive information to 3rd parties):
    a. contractually require all such 3rd parties to protect this information with safeguards at least as good as your own **Y / N / NA**
    b. perform due diligence on each such 3rd party to ensure that their safeguards for protecting sensitive information meet your standards (e.g. conduct security/privacy audits or review findings of independent security/privacy auditors) **Y / N / NA**
    c. Audit all such 3rd parties at least once per year to ensure that they continuously satisfy your standards for safeguarding sensitive information? **Y / N / NA**
    d. contractually require them to defend and indemnify you if they contribute to a confidentiality or privacy breach **Y / N / NA**
13. Do you have a way to detect unauthorized access or attempts to access sensitive information? **Y / N**
14. Do you retain Non-public Personal Information and others' sensitive information only for as long as needed and when no longer needed irreversibly erase or destroy same using a technique that leaves no residual information? **Y / N**
15. Do you know what sensitive or private information is in your custody along with whose info it is, where it is and how to contact individuals if their information is breached? **Y / N**
16. At least once a year, do you provide security awareness training for everyone who accesses your network or sensitive information in your care? **Y / N**
17. On your wireless networks; do you use security at least as strong as WPA authentication and encryption, and do you require two factor authentication (e.g. Some combination of VPN or Access token, and password/account logon) before allowing wireless connections to your network? (answer NA **ONLY** if you do not use wireless networks). **Y / N / NA**
18. a. Do your portable devices and removable media such as laptops, PDS, thumb drives, tapes or diskettes contain non-public personal or commercial information? **Y / N / N/A**
    If "yes", please attach a detailed description of the type of information contained on these devices.
    b. Do you encrypt personally identifiable information stored on portable devices and removable media and ensure that the encryption/decryption keys are not also stored on that device? **Y / N / N/A**

19. Similar to item 18 above, when transporting sensitive written records, do you ensure that the records are always under the direct physical control of an individual who has authorized access to the record (i.e. . record is never left unattended anywhere). Check NA **ONLY** if you never allow sensitive records to be removed from your premises. **Y / N / NA**
20. On your web-site, do you prominently display disclaimers & warnings on 3rd party privacy policies which may differ from your own wherever you provide links to such third party sites? Check NA **ONLY** if you do not link to 3rd party sites. **Y / N / NA**
21. Do you back-up your network data and configuration files daily and store back-up files in a secure location, and rehearse your procedure for restoring from back-ups at least yearly? **Y / N**
22. Do you have a written procedure that you rehearse at least yearly to ensure that you are proficient in responding to and recovering from network disruptions, intrusions, data loss and breaches of the following types:

    a. network attacks & incidents (including: malicious code, hacking, spy-ware) **Y / N**
    b. privacy/confidentiality breaches **Y / N**
    c. Denial of service attacks **Y / N**

23. Do you control and track all changes to your network to ensure that it remains secure? **Y / N**
24. Do you disallow all development activity (e.g. programming) and tools (e.g. compilers, linkers, assemblers and other development tools) on your production network? **Y / N**

AUTHORIZATION

I hereby acknowledge that the aforementioned statements and answers are correct and complete. I agree that any coverage issued will be contingent upon the truth of the preceding information. I further understand that any incorrect or incomplete statement could invalidate my coverage. I hereby authorize AAIC to release the information on this application and associated underwriting information.

FRAUD NOTICE

NOTICE TO FLORIDA APPLICANTS: Any person who knowingly and with intent to injure, defraud, or deceive any insurer files a statement of claim or an application containing any false, incomplete, or misleading information is guilty of a felony of the third degree.

_____

Signature in full Date

_____

Agent's Signature Date

If you apply your signature to this application electronically, you hereby consent and agree that your use of a key pad, mouse or other device to affect your electronic signature constitutes your signature, acceptance and agreement as if actually signed by you in writing and has the same force and effect as a signature affixed by hand.

This application is in compliance with Section 626.752, Florida Statutes. A copy has been furnished to the applicant or insured and coverage is:
[ ] Bound Effective (time) (date); [ ] Not Bound.

BROKER'S SIGNATURE:
Florida requires that we have the Name and Address of your (Applicant's) Authorized Agent or Broker.

Signature of Authorized Agent or Broker: _____

Name of Authorized Agent Broker: _____

Address:_____

License Identification Number: _____