

PARTNERSHIP. PREVENTION. PROTECTION.

This is an application for a CLAIMS-MADE AND REPORTED endorsement

Name of applicant \_\_\_\_\_ Policy number \_\_\_\_\_

1. Designated Privacy Officer or person who is responsible for privacy-related matters:

Name and title: \_\_\_\_\_ Phone number: \_\_\_\_\_

*PLEASE NOTE: if you answer "NO" to any items in Questions 2 - 5 below, please provide an explanation on the reverse side of this application or on a separate sheet.*

2. Is the applicant HIPAA compliant?

YES	NO
<input type="checkbox"/>	<input type="checkbox"/>

3. Does the applicant:

a) have an office/system-wide privacy policy to safeguard any and all individually identifiable patient information?

Check here if applicant/practice has no employees and continue to Question 4

b) require every current and new employee to be trained regarding the practice's privacy/confidentiality policy?

c) restrict employee access to patient files on a business need-to-know basis?

d) perform criminal background checks on new hires having access to protected, individually identifiable information?

<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

4. Regarding electronically stored or transmitted data/personal health information, does the applicant:

Check here if applicant/practice does not store or transmit any data or information electronically (e.g., billing, email, medical records, scheduling) and continue to Question 5

a) have a disaster recovery plan for the practice in place?

b) enforce security policies and procedures for firewalls on all internet access points?

c) use antivirus software on all computer systems, including laptops, personal computers and networks?

d) upgrade all security software regularly to account for new releases or improvements?

e) encrypt all electronic, protected, individually identifiable information on the applicant's computer hardware (including servers, laptops, smart phones, memory devices or personal digital assistants) or any other medium regardless of location:

i. while connected to the applicant's network?

ii. while disconnected from the applicant's network?

f) maintain procedures regarding the destruction of protected, individually identifiable information residing on systems or devices?

g) have separate user accounts per employee with defined password rules (e.g. case sensitive, alpha numeric)?

h) maintain formal processes to revoke network privileges immediately following an employee or independent contractor termination or resignation?

<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

5. Does the applicant shred all disposed paper containing protected, individually identifiable information?

*PLEASE NOTE: if you answer "YES" to question 6 or 7, please provide details on the reverse side of this application or on a separate sheet.*

6. Has the applicant:

a) ever received a claim alleging invasion of privacy, unauthorized disclosure, theft or loss of personal information, identity theft, breach of information security, or content infringement (such as trademark or copyright infringement) or been required to provide notification to individuals due to an actual or suspected disclosure of personal information?

b) been subject to any government action, investigation or subpoena regarding any alleged violation of any privacy or information security-related law or regulation?

YES	NO
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

7. Is the applicant aware of any fact or allegation which (a) might give rise to a claim against any proposed insured for invasion of privacy, unauthorized disclosure, loss or misuse of personal information; or (b) might require notifying patients of an actual or suspected disclosure of personal information?

<input type="checkbox"/>	<input type="checkbox"/>
--------------------------	--------------------------

All of the above information is true to the best of my knowledge and belief. I understand that signing this application does not bind Princeton Insurance Company to complete the insurance, but it is agreed that this application shall be the basis of a contract should an endorsement be issued. I understand that Princeton Insurance Company reserves the right to reject any applicant that does not meet its underwriting standards.

Signature of applicant \_\_\_\_\_ Date: \_\_\_\_\_

**NOTICE:** Any person who knowingly and with intent to defraud any insurance company or other person files an application for insurance or statement of claim containing any materially false information or conceals, for the purpose of misleading, information concerning any fact material thereto, commits a fraudulent insurance act, which is a crime and subjects such person to criminal and civil penalties.

Use the space below to provide details relative to the questions on the preceding page. If you need additional space, please provide additional pages and clearly indicate your name on each page.