



# BEAZLEY BREACH RESPONSE

## INFORMATION SECURITY & PRIVACY INSURANCE WITH BREACH RESPONSE SERVICES

**NOTICE: INSURING AGREEMENTS A., C., D. AND E. OF THIS POLICY PROVIDE COVERAGE ON A CLAIMS MADE AND REPORTED BASIS AND APPLY ONLY TO CLAIMS FIRST MADE AGAINST THE INSURED DURING THE POLICY PERIOD OR THE OPTIONAL EXTENSION PERIOD (IF APPLICABLE) AND REPORTED TO THE UNDERWRITERS DURING THE POLICY PERIOD OR AS OTHERWISE PROVIDED IN CLAUSE X, OF THIS POLICY. AMOUNTS INCURRED AS CLAIMS EXPENSES UNDER THIS POLICY SHALL REDUCE AND MAY EXHAUST THE LIMIT OF LIABILITY AND ARE SUBJECT TO RETENTIONS.**

**INSURING AGREEMENT B. OF THIS POLICY PROVIDES FIRST PARTY COVERAGE ON AN INCIDENT DISCOVERED AND REPORTED BASIS AND APPLIES ONLY TO INCIDENTS FIRST DISCOVERED BY THE INSURED AND REPORTED TO THE UNDERWRITERS DURING THE POLICY PERIOD.**

### PLEASE READ THIS POLICY CAREFULLY.

Please fully answer all questions and submit all requested information.

Full Name:			
Mailing Address:		State of Incorporation:	
City:		State & Zip:	
# of Employees:		Date Established:	
Website URL's:			
Authorized Officer <sup>1</sup> :		Telephone:	
		E-mail:	
Breach Response Contact <sup>2</sup> :		Telephone:	
		E-mail:	
<b>Applicant Business Activities:</b>			
1. Business Description:			
2. Does the Applicant provide data processing, data storage, or data hosting services to third parties? (If yes, please comment on the specific service in the description above.)		<input type="checkbox"/> Yes	<input type="checkbox"/> No
3. Does the Applicant distribute any products on a wholesale basis?		<input type="checkbox"/> Yes	<input type="checkbox"/> No
4. If yes, please confirm the percentage of revenue generated by wholesale distribution:		%	
<b>Revenue Information:</b>			
<b>*For Applicants in Healthcare: Net Patient Services Revenue plus Other Operating Revenue</b>			
<b>*For all other Applicants, please provide Gross Revenue information</b>			
	Most Recent Twelve (12) months: (ending: __/__/__)	Previous Year	Next Year (estimate)
US Revenue:	USD	USD	USD
Non-US Revenue:	USD	USD	USD
Total:	USD	USD	USD

<sup>1</sup> The officer of the Applicant that is designated to receive any and all notices from the Insurer or its authorized representative(s) concerning this insurance.

<sup>2</sup> The employee of the Applicant that is designated to manage a response, including consumer notification, in response to a data breach event.

**Please attach a copy of your most recently audited annual financial statement.**

Are significant changes in the nature or size of the Applicant's business anticipated over the next twelve (12) months? Or have there been any such changes within the past twelve (12) months?  Yes  No

If yes, please explain:

Has the Applicant within the past twelve (12) months completed or agreed to, or does it contemplate entering into within the next twelve (12) months, a merger, acquisition, consolidation, whether or not such transactions were or will be completed?  Yes  No

If yes, please explain:

**I. MANAGEMENT OF PRIVACY EXPOSURES**

- 1. Has the Applicant designated a Chief Privacy Officer?  Yes  No  
If no, please indicate what position (if any) is responsible for privacy issues:
- 2. Does the Applicant have a written corporate-wide privacy policy?  Yes  No  
If yes, please attach a copy of the privacy policy to this application.
- 3. Is the Applicant in compliance with its privacy policy?  Yes  No  
If no, please provide details regarding such non-compliance:
- 4. Does the Applicant accept credit cards for goods sold or services rendered?  Yes  No  
If yes:
  - A. Please state the Applicant's approximate percentage of revenues from credit card transactions in the most recent twelve (12) months: %
  - B. Is the Applicant compliant with applicable data security standards issued by financial institutions the Applicant transacts business with (e.g. PCI standards)?  Yes  No  
If the Applicant is not compliant with applicable data security standards, please describe the current status of any compliance work and the estimated date of completion:
- 5. Does the Applicant restrict employee access to personally identifiable on a business-need to know basis?  Yes  No
- 6. Does the Applicant require third parties with which it shares personally identifiable information or confidential information to indemnify the Applicant for legal liability arising out of the release of such information due to the fault or negligence of the third party?  Yes  No
- 7. Has the Applicant implemented an identity theft prevention program (aka FTC "Red Flags" program)?  Yes  No
- 8. If the Applicant is in the healthcare industry, does the Applicant host, operate, or manage a Healthcare Information Exchange on which other organizations may store personal health information?  Yes  No

**II. COMPUTER SYSTEMS CONTROLS**

- 1. Has the Applicant designated a Chief Security Officer as respects computer systems?  Yes  No  
If no, please indicate what position is responsible for computer security:
- 2. Does the Applicant publish and distribute written computer and information systems policies and procedures to its employees?  Yes  No
- 3. Does the Applicant conduct training for every employee user of the information systems in security issues and procedures for its computer systems?  Yes  No
- 4. Does the Applicant have :

<p>A. a disaster recovery plan?</p> <p>B. a business continuity plan?</p> <p>C. an incident response plan for network intrusions and virus incidents?</p> <p>How often are such plans tested?</p>	<input type="checkbox"/> Yes	<input type="checkbox"/> No																
<p>5. Does the Applicant have a program in place to test or audit security controls on an annual or more frequent basis?</p> <p>If yes, please summarize the scope of such audits and/or tests:</p>	<input type="checkbox"/> Yes	<input type="checkbox"/> No																
<p>6. Does the Applicant terminate all associated computer access and user accounts as part of the regular exit process when an employee leaves the company?</p>	<input type="checkbox"/> Yes	<input type="checkbox"/> No																
<p>7. Is all valuable/sensitive data backed-up by the Applicant on a daily basis?</p> <p>If no, please describe exceptions:</p>	<input type="checkbox"/> Yes	<input type="checkbox"/> No																
<p>8. Is at least one complete back-up file generation stored and secured off-site separate from the Applicant's main operations in a restricted area?</p> <p>If no, describe the procedure used by the Applicant, if any, to store or secure copies of valuable/sensitive data off-site?</p>	<input type="checkbox"/> Yes	<input type="checkbox"/> No																
<p>9. Does the Applicant have and enforce policies concerning when internal and external communication should be encrypted?</p> <p>A. Are users able to store data to the hard drive of portable computers or portable media devices such as USB drives?</p> <p>B. Does the Applicant encrypt data stored on laptop computers and portable media?</p> <p>C. Please describe any additional controls the Applicant has implemented to protect data stored on portable devices:</p>	<input type="checkbox"/> Yes	<input type="checkbox"/> No																
<p>10. What format does the Applicant utilize for backing up and storage of computer system data?</p> <p><input type="checkbox"/> Tape or other media    <input type="checkbox"/> Online backup service    <input type="checkbox"/> Other:</p> <p>A. Are tapes or other portable media containing backup materials encrypted?</p> <p>B. Are tapes or other portable media stored offsite using secured transportation and secured storage facilities?</p> <p>    1) If stored offsite, are transportation logs maintained?</p> <p>If stored onsite, please describe physical security controls:</p>	<input type="checkbox"/> Yes	<input type="checkbox"/> No																
<p>11. Does the Applicant enforce a software update process including installation of software "patches"?</p> <p>If Yes, are critical patches installed within thirty (30) days of release?</p>	<input type="checkbox"/> Yes	<input type="checkbox"/> No																
<p>12. Please describe your network infrastructure:</p> <table style="width: 100%; border: none;"> <tr> <td style="width: 25%;"></td> <td style="width: 15%; text-align: center;"><b>Anti-virus</b></td> <td style="width: 15%; text-align: center;"><b>Firewall</b></td> <td style="width: 15%; text-align: center;"><b>ISP</b></td> <td style="width: 20%; text-align: center;"><b>Intrusion Detection</b></td> </tr> <tr> <td><b>Primary vendor:</b></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td><b>Other significant vendor:</b></td> <td></td> <td></td> <td></td> <td></td> </tr> </table>		<b>Anti-virus</b>	<b>Firewall</b>	<b>ISP</b>	<b>Intrusion Detection</b>	<b>Primary vendor:</b>					<b>Other significant vendor:</b>							
	<b>Anti-virus</b>	<b>Firewall</b>	<b>ISP</b>	<b>Intrusion Detection</b>														
<b>Primary vendor:</b>																		
<b>Other significant vendor:</b>																		
<p>13. How often are virus signatures updated?</p> <p><input type="checkbox"/> Automatic Updates    <input type="checkbox"/> Weekly    <input type="checkbox"/> Monthly    <input type="checkbox"/> Other</p>																		
<p>14. Does the Applicant require computer service providers who may have access to confidential information or personally identifiable information to demonstrate adequate security policies and procedures?</p> <p>A. Are computer service providers required by contract to indemnify the Applicant for harm arising from a breach of the provider's security?</p>	<input type="checkbox"/> Yes	<input type="checkbox"/> No																

**III. WEBSITE CONTENT CONTROLS**

1. Please check all descriptions of website content posted by the Applicant, including content posted to social media web pages:

No Website
  Information created by the Applicant  
 Content under license from a third party
  Streaming video or music content  
 Unlicensed third party content (e.g. – Blog/Message Boards/ Customer Reviews)

2. Does the Applicant have a procedure for responding to allegations that content created, displayed or published by the Applicant is libelous, infringing, or in violation of a third party's privacy rights?  Yes  No

3. Does the Applicant have a process to review all content prior to posting on the Insured's Internet Site or on social media web pages created and maintained by or on behalf of the Insured?  Yes  No

If yes: is the review performed by a qualified attorney?  Yes  No

Does the review include screening the content for the following:

A. disparagement issues?  Yes  No

B. copywriting infringement?  Yes  No

C. trademark infringement?  Yes  No

D. invasion of privacy?  Yes  No

If the Applicant does not have a process to review all content prior to posting, please describe procedures to avoid the posting of improper or infringing content:

4. Has the Applicant screened all trademarks used by the Applicant for infringement with existing trademarks prior to first use?  Yes  No

A. Has the Applicant acquired any trademarks from others in the past three (3) years?  Yes  No

If Yes, were acquired trademarks screened for infringement?  Yes  No

**IV. PRIOR INSURANCE**

1. Does the Applicant currently have insurance in place covering media, privacy or network security exposures?  Yes  No

If yes, please provide the following:

Insurer	Limits	Deductible	Policy Period	Premium	Retroactive Date

2. Has any professional liability, privacy, network security or media insurance ever been declined or cancelled?  Yes  No

If yes, please provide details:

**V. PRIOR CLAIMS AND CIRCUMSTANCES**

1. Does the Applicant or other proposed insured, or any director, officer or employee of the Applicant or other proposed insured have knowledge of or information regarding any fact, circumstance, situation, event or transaction which may give rise to a claim or loss or obligation to provide breach notification under the proposed insurance?  Yes  No

If yes, please provide details:

2. During the past 5 years has the Applicant:

A. received any claims or complaints with respect to privacy, breach of information or network security, unauthorized disclosure of information, or Yes No



FOR COMMERCIAL OR PERSONAL INSURANCE WHICH SUCH PERSON KNOWS TO CONTAIN MATERIALLY FALSE INFORMATION CONCERNING ANY FACT MATERIAL THERETO; OR CONCEALS, FOR THE PURPOSE OF MISLEADING, INFORMATION CONCERNING ANY FACT MATERIAL THERETO COMMITS A FRAUDULENT INSURANCE ACT.

**NOTICE TO KENTUCKY, NEW JERSEY, NEW YORK, OHIO AND PENNSYLVANIA APPLICANTS:** ANY PERSON WHO KNOWINGLY AND WITH INTENT TO DEFRAUD ANY INSURANCE COMPANY OR OTHER PERSON FILES AN APPLICATION FOR INSURANCE OR STATEMENT OF CLAIMS 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. (IN NEW YORK, THE CIVIL PENALTY IS NOT TO EXCEED FIVE THOUSAND DOLLARS (\$5,000) AND THE STATED VALUE OF THE CLAIM FOR EACH SUCH VIOLATION.)

**NOTICE TO MAINE, TENNESSEE, VIRGINIA AND WASHINGTON APPLICANTS:** IT IS A CRIME TO KNOWINGLY PROVIDE FALSE, INCOMPLETE OR MISLEADING INFORMATION TO AN INSURANCE COMPANY FOR THE PURPOSE OF DEFRAUDING THE COMPANY. PENALTIES MAY INCLUDE IMPRISONMENT, FINES OR A DENIAL OF INSURANCE BENEFITS.

**NOTICE TO MARYLAND APPLICANTS:** ANY PERSON WHO KNOWINGLY OR WILLFULLY PRESENTS A FALSE OR FRAUDULENT CLAIM FOR PAYMENT OF A LOSS OR BENEFIT OR KNOWINGLY OR WILLFULLY PRESENTS FALSE INFORMATION IN AN APPLICATION FOR INSURANCE IS GUILTY OF A CRIME AND MAY BE SUBJECT TO FINES AND CONFINEMENT IN PRISON.

**NOTICE TO OKLAHOMA APPLICANTS:** WARNING: ANY PERSON WHO KNOWINGLY, AND WITH INTENT TO INJURE, DEFRAUD OR DECEIVE ANY INSURER, MAKES ANY CLAIM FOR THE PROCEEDS OF AN INSURANCE POLICY CONTAINING ANY FALSE, INCOMPLETE OR MISLEADING INFORMATION IS GUILTY OF A FELONY.

### **SIGNATURE SECTION**

THE UNDERSIGNED AUTHORIZED EMPLOYEE OF THE APPLICANT DECLARES THAT THE STATEMENTS SET FORTH HEREIN ARE TRUE. THE UNDERSIGNED AUTHORIZED EMPLOYEE AGREES THAT IF THE INFORMATION SUPPLIED ON THIS APPLICATION CHANGES BETWEEN THE DATE OF THIS APPLICATION AND THE EFFECTIVE DATE OF THE INSURANCE, HE/SHE WILL, IN ORDER FOR THE INFORMATION TO BE ACCURATE ON THE EFFECTIVE DATE OF THE INSURANCE, IMMEDIATELY NOTIFY THE UNDERWRITER OF SUCH CHANGES, AND THE UNDERWRITER MAY WITHDRAW OR MODIFY ANY OUTSTANDING QUOTATIONS OR AUTHORIZATIONS OR AGREEMENTS TO BIND THE INSURANCE. FOR NEW HAMPSHIRE APPLICANTS, THE FOREGOING STATEMENT IS LIMITED TO THE BEST OF THE UNDERSIGNED'S KNOWLEDGE, AFTER REASONABLE INQUIRY. IN MAINE, THE UNDERWRITERS MAY MODIFY BUT MAY NOT WITHDRAW ANY OUTSTANDING QUOTATIONS OR AUTHORIZATIONS OR AGREEMENTS TO BIND THE INSURANCE.

NOTHING CONTAINED HEREIN OR INCORPORATED HEREIN BY REFERENCE SHALL CONSTITUTE NOTICE OF A CLAIM OR POTENTIAL CLAIM SO AS TO TRIGGER COVERAGE UNDER ANY CONTRACT OF INSURANCE. NO COVERAGE SHALL BE AFFORDED FOR ANY CLAIMS ARISING OUT OF A CIRCUMSTANCE NOT DISCLOSED IN THIS APPLICATION.

SIGNING OF THIS APPLICATION DOES NOT BIND THE APPLICANT OR THE UNDERWRITER TO COMPLETE THE INSURANCE, BUT IT IS AGREED THAT THIS APPLICATION SHALL BE THE BASIS OF THE CONTRACT SHOULD A POLICY BE ISSUED, AND IT WILL BECOME PART OF THE POLICY.

ALL WRITTEN STATEMENTS AND MATERIALS FURNISHED TO THE INSURER IN CONJUNCTION WITH THIS APPLICATION ARE HEREBY INCORPORATED BY REFERENCE INTO THIS APPLICATION AND MADE A PART HEREOF. FOR NORTH CAROLINA, UTAH, AND WISCONSIN APPLICANTS, SUCH APPLICATION MATERIALS ARE PART OF THE POLICY, IF ISSUED, ONLY IF ATTACHED AT ISSUANCE.

Signed\*: \_\_\_\_\_

Date: \_\_\_\_\_

Print Name: \_\_\_\_\_  
(Owner, Partner, Authorized Officer)

Title: \_\_\_\_\_

If this **Application** is completed in Florida, please provide the Insurance Agent's name and license number. If this **Application** is completed in Iowa or New Hampshire, please provide the Insurance Agent's name and signature only.

Agent's Printed Name: \_\_\_\_\_

Florida Agent's License Number: \_\_\_\_\_

Agent's Signature\*: \_\_\_\_\_