Admiral
INSURANCE GROUP
a Berkley Company

ADMIRAL VIRTUAL CARE PROFESSIONAL LIABILITY APPLICATION AND GENERAL LIABILITY APPLICATION

SECTION I – GENERAL INFORMATION

1. Full Name of Applicant:
   (Include all prior names, DBAs and subsidiaries seeking coverage under the policy for which you are applying)

2. Mailing & Location Address (If multiple locations, include an attachment with a complete list of locations):

   Mailing:

   Location:

3. Website Address(es):
4. Date Established (mm/dd/yy):
5. FEIN:
6. Are you owned by, associated with, or controlled by any other entity or are you part of a franchise? Yes No
   If Yes, describe:

7. Have you experienced any mergers, acquisitions, or divestitures in the last 5 years? Yes No

   Do you plan on any within the next 12 months? Yes No
   If Yes to either of the above, provide complete details:

8. Does the Applicant own, operate, or manage any business other than the one(s) described in this application for which you are applying for coverage? Yes No
   If Yes, provide complete details including name of entity, your ownership interest or contractual relationship, and information on their insurance program(s):

SECTION II – GETTING TO KNOW YOU

9. In your own words, describe your technology and medical services/products:

10. Describe the most likely result if your product or service failed to perform as intended:

11. Complete all sections that apply:

	Total Revenue	# of Outpatient Visits	# of Inpatient Beds	# of Non-Emergency Transports	# of Emergency Transports	# of Students	# of Surgeries
Next 12 Months	$						
Last 12 Months	$						
Two Years Ago	$						

12. Provide the percentage (%) of Total Revenue attributed to foreign locations/operations: %
    If greater than 0%, provide details including list of countries, number of employees in each and percentage of revenue associated with each country:

13. In the last fiscal year, what percentages of your revenue were from the following technology activities:
    (Total must equal 100%)

Technology Activities	Revenue %
Software	
Custom Healthcare Software Development and Licensing	%
General Wellness Mobile Application or Platform Provider	%
Health Information Exchange (EHR)	%
Healthcare Call Center Platform	%
Healthcare Patient Portal – Account Management	%
Online Prescription Coordination Services	%
Remote Patient Monitoring Software	%
Telehealth Platform – Remote Patient Consultations	%
Teleradiology Services	%
Hardware/Products	
Design, Distribution, or Licensing of Laboratory or Diagnostic Testing Kits	%
Medical Technology Product Design & Distribution – No Patient Monitoring	%
Medical Technology Product Design & Distribution – General Wellness Patient Monitoring	%
Medical Technology Product Design & Distribution – Critical Care Patient Monitoring	%
Technology Resellers	
Value-Added Reseller of Non-Proprietary Hardware	%
Value-Added Reseller of Non-Proprietary Software	%

Technology Activities	Revenue %
Other Services	
Healthcare Software & Hardware Installation & Integration Services – Not Proprietary	%
Healthcare Technology Consulting	%
Medical Billing Platform and Other Billing Services	%
Network Security Consulting & Security Audits (no real time monitoring)	%
Privacy Law/HIPAA Compliance Consulting	%
Staffing – Healthcare (All Other)	%
Staffing – Healthcare (Hospital Based)	%
Staffing – Technology	%
Other:	%

14. For the above technology services and/or products you provide, select which healthcare/medical services they support (Check all that apply):

    General Wellness & Fitness and Consulting

    Medical Spa Services

    Outpatient Clinic Services

    Primary Care/General Care Services

    Imaging Services

    Laboratory Services

    Substance Abuse / Behavioral Health Treatment

    Online Pharmacy Services with Limited to No Controlled Substance Exposure

    Online Pharmacy Services with Controlled Substances Over 25%

    Inpatient Facility

    Pediatric Patients

    Senior Care Patients

    Hospitals Patients/Systems

    Vital Care Monitoring Services

    Patient Diagnosis

    Patient Treatment Plan Development

    Surgical Procedures

    Other (describe):

15. List your five largest contracts in the last three years.

Client	Services Rendered	Project Duration	Revenue Derived
			$
			$
			$
			$
			$

16. For your **Non-Medical Personnel**, complete the following employee breakdown as applicable:

	Number of Employees
Technology Development Personnel	
Administrative Personnel	
Sales & Marketing	
Other:	

17. For your **Medical Personnel**, complete the following employee breakdown as applicable:

	Number of Employees	Number of Independent Contractors*	Insured on Own Med Mal Policy	Current Carrier & Limits of Liability
Physicians (no surgery)			Yes No	
Physicians (surgical)			Yes No	
Physician Assistants			Yes No	
Nurse Practitioners / APRNs			Yes No	
CRNAs			Yes No	
Surgical Technicians			Yes No	
Nurses (RN/LPN/LVN)			Yes No	
Aestheticians			Yes No	
Laser Techs			Yes No	
Medical Assistants			Yes No	
Massage Therapists			Yes No	
Pharmacists			Yes No	
Paramedics/EMT's			Yes No	
Social Workers/LMT/Counselors			Yes No	
Physical/Speech/Occupational Therapists			Yes No	
Other:			Yes No	

* Attach copies of declaration pages on all individuals that carry their own malpractice.

Would you like to include coverage for any physician's, dentist's, surgeon's, podiatrist's or chiropractor's direct patient care? Yes No
If Yes, have each Physician complete the Admiral Physicians and Surgeons Short Form Application.

18. Provide details for any services you subcontract out to others, including percentage of revenue:

19. Do you have a Medical Director? Yes No
    a. If Yes, provide their name and medical designation:
    b. What is the Medical Director's medical specialty?
    c. Does the Medical Director provide good faith exams or develop treatment plans? Yes No
    d. Would you like to include coverage for the Medical Director's supervisory duties over PA-c, NP, or APRNs at this facility? Yes No

e. Would you like to include coverage for the Medical Director's direct patient care? Yes No
If Yes, have each Physician complete the Admiral Physicians and Surgeons Short Form Application.

20. Explain your credentialing process for all providers, including primary source verification and reference checks:

21. Are background checks performed on all employees, independent contractors, and volunteers? Yes No
If Yes, what level or type of criminal background checks?

County State Federal Sexual Offender Registry

If No, provide details:

22. Are all employees, independent contractors and volunteers screened for drugs and alcohol? Yes No

If Yes, how often are screens performed?

23. Do you have a policy to prevent sexual abuse or allegations of sexual abuse? Yes No
If Yes, describe and advise how often it is reviewed:

24. Does your practice include prescribing of opioids? Yes No

If Yes, provide the following details:

a. Specify the percentage of your practice derived from opioid prescriptions: %

b. Do you fully comply with the CDC Guideline for Prescribing Opioids? Yes No

c. Does your practice adhere to any and all prescription drug monitoring program (PDMP) requirements in the state(s) where you conduct business? Yes No

d. Do you also dispense the opioids? Yes No

25. In the past twelve (12) months or next twelve (12) months projected, has the applicant or is the applicant planning on administering any Non-Invasive Weight Loss treatment (i.e. Semaglutide)? Yes No
If Yes, complete the Non-Invasive Weight Loss Supplemental Application and provide the informed consent specific to non-invasive weight loss used.

26. For inpatient services, provide the following, if applicable: N/A Yes No

a. Do you provide rapid detox under anesthesia services? Yes No

b. For inpatient beds, provide the average length of stay:

c. Provide the medical staff to bed ratio breakdown along with the shift structure and hours below:

8-Hour Shift Structure	**Staff: Resident Ratio**	**12-Hour Shift Structure**	**Staff: Resident Ratio**
7:00am – 3:00pm		7:00am – 7:00pm	
3:00pm – 11:00pm		7:00pm – 7:00am	
11:00pm – 7:00am			

27. Provide percentage breakdown for the location(s) your services are provided (total must equal 100%):

%	Location
%	Patient's Home
%	Clinic, Hospital or Physician's Office
%	Virtually (online platform, telephone, etc.)
%	Nursing Home
%	Assisted Living Facility
%	Jails or Correctional Facilities
%	Other (explain):

28. Provide percentage breakdown of patient population (total must equal 100%):

Check if not applicable.

%	Ages
%	Ages 0 – 17
%	Ages 18 – 59
%	Ages 60+

29. Indicate the percentage or number of patient encounters for each state (if using percentage, total must equal 100%):

Check if not applicable.

State	Percent	Number	State	Percent	Number	State	Percent	Number	State	Percent	Number
AL	%		IA	%		MT	%		RI	%	
AK	%		IL	%		NE	%		SC	%	
AZ	%		IN	%		NV	%		SD	%	
AR	%		KS	%		NH	%		TN	%	
CA	%		KY	%		NJ	%		TX	%	
CO	%		LA	%		NM	%		UT	%	
CT	%		ME	%		NY	%		VT	%	
DC	%		MD	%		NC	%		VA	%	
DE	%		MA	%		ND	%		WA	%	
FL	%		MI	%		OH	%		WV	%	
GA	%		MN	%		OK	%		WI	%	
HI	%		MS	%		OR	%		WY	%	
ID	%		MO	%		PA	%				

SECTION III – TECHNOLOGY RISK MANAGEMENT

(*Answer all that apply)

30. Is all software development work documented and tested before deployment? Yes No

31. If you host a software application for clients, do you have a secondary backup that can be used in the event of an outage to the application? Yes No
    If Yes:
    a. Is that back-up stored on an off-site server at a separate location? Yes No
       If No, where is the back-up stored?
    b. Have you tested the successful restoration of the backup application in the last year? Yes No

c. Describe any other aspects of your security, testing and recovery procedures around the client environment:

32. If your technology monitors or supports critical patient care, describe backup procedures for immediate patient care in the event of an outage or disruption to the software or technology product until such outage or disruption is resolved:

33. If you provide any proprietary technology hardware products as part of your offering to clients, complete the following:

    a. Provide the name of the third-party manufacturer of your product:

    b. Describe vetting procedures for selecting the manufacturer:

    c. Do you execute a written contract or agreement with every third-party manufacturer that you use? Yes No

    d. Do you require your third-party manufacturer to carry either or both of the following (check all that apply):

        Professional Liability Insurance

        Commercial General Liability insurance

34. Have any of your products or third-party products you provide to clients been subject to a product recall? Yes No
    If Yes, provide details including product recall costs to you, the remedy and if any third-party claims or litigation related to the product recall:

35. Have you discontinued any software, product, or service in the last five years? Yes No
    If Yes, provide details including whether you continued to provide maintenance and software patching services:

SECTION IV – NETWORK SECURITY & DATA PRIVACY

PART 1 – INTERNAL TRAINING, POLICIES AND PROCEDURES

36. Do you conduct employee training on an annual basis (or more frequently) related to:

    a. HIPAA Compliance Yes No

    b. Company Incident Reporting Procedures Yes No

    c. Document Management Yes No

    d. Internet and Email Use Yes No

    e. Passwords Yes No

    f. Responsibility for Company Data Yes No

37. Do you conduct cyber competency testing on an annual basis (or more frequently) for employees and contractors on:

a. Social engineering attacks (i.e. email-based phishing, baiting, scareware, etc.) Yes No

b. Physical security (locked and secured computer devices) Yes No

38. Do you use any of the following technology:

a. Meta Pixel or similar technology on your website Yes No

b. Session Replay or similar technology Yes No

c. Chatbot or similar technology Yes No

If Yes to any of the above, do you request affirmative consent from users? Yes No
If No, describe below:

39. Do you have rapid (immediate) account access termination procedures for employees that leave the company? Yes No

40. Do you have a privacy policy? Yes No

If Yes, has it been reviewed by legal representation? Yes No

41. Do you maintain an incident response plan which includes business continuity mitigation procedures in the event of a ransomware threat? Yes No

42. a. Are you compliant with the following:

	Indicate N/A, Yes or No	Date of Last Audit/Assessment
Health Information Portability and Accountability Act (HIPAA)	N/A Yes No	
Health Information Technology for Economic and Clinical Health Act (HITECH)	N/A Yes No	
Payment Card Industry Data Security Standards (PCI DSS)	N/A Yes No	

b. If you are subject to PCI DSS, what is your certification level?

c. Complete the chart below for any of the following assessments you have completed:

	Indicate N/A, Yes or No	Date of Last Audit/Assessment
SOC II Certification Type I	N/A Yes No	
SOC II Certification Type II	N/A Yes No	
Biometric Information Privacy Act (BIPA)	N/A Yes No	

d. Describe any changes made to operations, procedures and/or network security and data privacy practices as a result of the recent Audits/Assessments listed in the two charts above:

PART 2 – NETWORK SECURITY AND DATA PRIVACY CONTROLS

43. a. Where do your servers reside? Cloud On Premises

    b. If cloud, which vendor(s) do you use?

    c. Are your production servers separated in different locations? Yes No

44. a. Is your network managed in-house or by a vendor?

    b. If outsourced, which vendor(s) do you use?

    c. What are the qualifications of your IT security leaders? (Examples: CISSP, CISM, CISA, CEH, CCSP)

45. Indicate all IT risk management elements implemented:

	In-House	Vendor		In-House	Vendor
Access Restrictions			Hot Site		
Anti-Virus Scanning			Load Balancers		
Automated Security Scanning			Proxy Servers		
Network Intrusion Detection			Security Audits		
Encryption			Secure Remote Capabilities		
Firewall			Others:		

46. What types of network monitoring solutions (active and passive) do you have in place, and who does the monitoring?

47. How frequently do you test your network security to ensure effectiveness and response time?

    Monthly Quarterly Annually

48. What are your procedures for correcting vulnerabilities from penetration testing?

49. a. How often do you patch:

    Server infrastructure:

    Desktop/laptop infrastructure:

    b. If you are a software company, how often do you issue patches?

    c. Are you responsible for patching any systems for customers? Yes No

    If Yes, how frequently?

    d. How do you respond to Zero-Day vulnerabilities? *(A Zero-Day vulnerability or exploit is a vulnerability that has been disclosed but not yet patched. Recent example: log4j.)*

50. Do you employ Endpoint Detection and Response (EDR) security tools? Yes No

51. Do you employ network segmentation to separate critical systems, applications, and data from non-critical? Yes No

52. Do you employ Multi-Factor Authentication for the following:

a. Critical Information Yes No

b. Remote Access Yes No

c. Administrator and privileged user accounts Yes No

d. Personal devices accessing the network Yes No

e. Independent contractor and vendors accessing the network Yes No

f. Non-critical information and applications Yes No

53. a. Are workstations prohibited from local admin rights? Yes No

b. If Yes, all the time or case by case?

c. Do you manage privileged accounts using tooling such as CyberArk or other? Yes No

d. How many users have persistent privileged accounts for endpoints (defined as those who have entitlements to configure, manage, and support endpoints)?

Describe compensating security controls for these specific persistent privileged accounts:

54. Do you route all outbound web requests through a web proxy which monitors for and blocks potentially malicious content? Yes No

55. Are external emails tagged as such to alert your employees that the email originated from outside of your organization? Yes No

56. Do you utilize Microsoft Office 365? Yes No

If Yes, does this include Office 365 Threat Protection add-on? Yes No

If No, or if you use an alternate product to MS Office 365, provide details or an explanation as to why this measure has not been implemented:

57. Provide the estimated record count of sensitive information you maintain on your servers, store with a cloud provider and host for others:

	Number of Records
Medical Records	
Medical Records Attributed to Minors	
Financial Records (credit/debit cards, bank account #'s, etc.)	
Other Protected Personally Identifiable Information	
TOTAL RECORD COUNT	

58. Do you require encryption for the following:

a. Sensitive information while in transit? Yes No

b. Sensitive information while at rest? Yes No

c. Remote Access Yes No

d. How are your encryption keys protected?

59. a. How often do you purge data?

b. Check the following safeguards that you use for data destruction:

Physical Destruction – Certification from vendor for physical shredding of media.

Overwriting – Single or multiple overwriting passes with fixed pattern such as binary zeroes.

Degaussing – Strong magnetic field applied to magnetic media to randomize field orientation.

60. How do you ensure sensitive data destruction compliance with applicable privacy law?

61. What are your data security vetting procedures for third parties that you either share data or network access to?

62. Do you use any physical security controls to prevent unauthorized access to networks and data? (Examples: controlled swipe card access with logging, security cameras, etc.) Yes No
If Yes, describe such controls:

PART 3 – BACKUP AND RECOVERY

63. a. How often are network backups performed?

b. How often are these backups tested?

c. Are the backups stored offsite? Yes No

d. Are backup files encrypted? Yes No

64. Is backup access subject to separate authorization credentials which are maintained separately from common system credentials? Yes No

65. Do you test the successful restoration and recovery of key server configurations and data from backups? Yes No

If Yes, how often?

66. a. How often is your disaster recovery plan tested?

b. What is your recovery time objective? (This is the time it takes to recover from an event.)

c. What is your recovery point objective? *(This is the point in time to which you are restoring or how far back in time prior to an event that the last known backup or last known good configuration is known to exist.)*

PART 4 – CYBER CRIME

67. Is dual authorization required for all wire transfers? Yes No
    If Yes, describe authorization process including which employees or departments have the authority to do so:

68. Are transfer verifications sent to an employee or department other than the one that initiated the transfer? Yes No

69. For employees responsible for wire transfers, is training conducted regarding common wire transfer fraud attack vectors (i.e. social engineering phishing, spear phishing, whaling)? Yes No

    If Yes, how often?

70. Do you call to verify or have another verification process if a client or vendor makes a request via email to change bank account information or key information for future invoices? Yes No
    If Yes, describe:

SECTION V – MEDIA

71. Do you use media content provided by others? Yes No
    If Yes, describe:

72. Describe your procedures for removing defamatory, infringing, or damaging content from your website and mobile applications:

73. Do you send any electronic advertising content to outside parties regarding your products or services or the products or services of your clients? Yes No
    If Yes, what media do you use for such advertising?

    SMS Text Messaging

    Phone Calls

    Email

    Others:

74. Do you always obtain the appropriate permission from recipients of your advertisements when such permission is required by law? Yes No

75. Do your websites allow for others to upload or otherwise share content with others? Yes No

SECTION VI – COVERAGE HISTORY

76. Provide details of your most recent coverage for Professional Liability, Cyber Liability and General Liability. Attach copies of expiring Declarations pages evidencing prior limits and retroactive dates.

	Carrier	Limit	Deductible	Policy Term	Retroactive Date
Professional Liability					
Cyber Liability					
General Liability					

*If General Liability is purchased, is it on:

Claims Made CGL Form

Occurrence CGL Form

77. Are you interested in a quote for General Liability? Yes No

If Yes, complete the General Liability Supplemental Application below or submit a signed GL Acord Application.

SECTION VII – CLAIMS HISTORY

PROVIDE 5 YEARS OF CURRENTLY VALUED LOSS RUNS.

78. Have any of the Applicant's employee(s) or independent contractors been the subject(s) of alleged or actual incidents regarding sexual abuse or molestation or child abuse/neglect? Yes No

If Yes, provide details on a separate attachment.

79. Has the applicant or any of the above employees and/or independent contractors:

a. Ever been subject to a disciplinary or investigative proceeding or been reprimanded by a government or administrative agency, hospital, or professional association? Yes No

b. Ever been convicted of a criminal act other than traffic offenses? Yes No

c. Ever been treated for alcoholism or drug addiction? Yes No

d. Ever had any professional license or license to prescribe or dispense narcotics refused, suspended, revoked, renewal refused or accepted only on special terms, or ever voluntarily surrendered such license? Yes No

If Yes to any of the above questions, describe:

80. Has any insurer declined, cancelled or non-renewed any similar insurance for which you are applying? Yes No
If Yes, provide complete details:

81. After inquiry, is the applicant, any predecessor, or any other person for whom coverage is requested been subject to any actions or investigations by any regulatory or administrative body for violations arising out of your advertising or electronic communication activities? Yes No
If Yes, provide complete details:

82. Have any claims, suits or regulatory proceedings ever been made against the Applicant or any of its employees? Yes No
If Yes, complete a Supplemental Claim Information Form for each and every claim.

83. Is the applicant aware of any errors, omissions, circumstances, or incidents which may result in a claim being made against them or their employees, or are there any claims that have not yet been reported? Yes No
If Yes, provide complete details:

84. In the past five (5) years:

a. Have you experienced any:

i. Known intrusions (i.e. unauthorized access), security incidents, security breaches or cyber-attacks? Yes No

ii. Actual or attempted extortion demand with respect to your computer systems? Yes No

iii. Unexpected outage of a computer network, application, or system lasting greater than four (4) hours? Yes No

b. Have you experienced an actual or suspected data breach or cyber-attack? Yes No
If Yes, provide a detailed description of the event(s) and remediation action(s) taken:

c. Have you received any complaints concerning the content of your websites or electronic communications? Yes No
If Yes, provide complete details:

d. Have you been accused of, made aware of, or had a claim as a result of actual or alleged infringement upon another's domain name, trademark, copyright, services mark or similar intellectual property? Yes No
If Yes, provide complete details:

*For each and every claim, click the link to complete the Supplemental Claim Information Form.

SECTION VIII – COMMENTS

Use this space below to provide us with any other relevant information:

GENERAL LIABILITY SUPPLEMENTAL APPLICATION

If you want GL coverage, complete the following or submit a signed GL Acord Application.

SECTION I – YOUR LOCATIONS

IF YOU HAVE MORE THAN FIVE (5) LOCATIONS, PROVIDE A SPREADSHEET WITH THE INFORMATION BELOW FOR EACH LOCATION.

1.

Loc #	Facility Name	Address	Description / Use	Square Footage	How many other occupants do you share the building with?
1					
2					
3					
4					
5					

SECTION II – FIRE-LIFE SAFETY INFORMATION

2. Are all of your locations equipped with:
   a. Complete sprinkler system? Yes No
   b. At least two clearly marked exits on each floor? Yes No
   c. Smoke detectors? Yes No
   d. Emergency electrical system? Yes No
   e. Heat sensors? Yes No
   f. Fire escape(s)? Yes No
   g. Posted emergency evacuation procedures? Yes No
   h. Properly maintained fire extinguishers? Yes No

SECTION III – PRODUCTS

PART 1 – EQUIPMENT SOLD OR LEASED

3. Do you loan, lease or rent equipment to others? Yes No
   a. Annual gross revenue **for equipment rental**? $
   b. With or without operator (technician)? With Without
      Provide details:
   c. Who is responsible for equipment maintenance?

4. Do you sell durable medical equipment? Yes No
   If Yes, provide the Medical Equipment Suppliers Revenue below:

	Annual Sales	Annual Lease/Rental
Category I: Expendable Items (i.e. adhesive tape, bandages, hypodermic needles)	$	$
Category II: Non-Expendable Items (i.e. hospital beds, bathroom safety bars, canes, walkers, wheelchairs, crutches, IV stands, etc.)	$	$
Category III: Diagnostic or Treatment Devices (i.e. oxygen, IV pumps, blood pressure gauges, transmitting devices)	$	$
Category IV: Life Sustaining or Critical Life Monitoring Equipment or Devices (i.e. dialysis machines, heart/lung machines, ventilators, etc.)	$	$

PART 2 – PRODUCTS & COMPLETED OPERATIONS

Attach a separate sheet detailing any Yes answers, along with a list of products sold.
If product labels cannot be found on your website, include copies with this application.

5. Do you sell any physical products? Yes No
   If No, skip to question 20.

   Describe the types of products you sell:

6. Advise total gross revenue **from product sales**:
   a. Last twelve (12) months: $
   b. Next twelve (12) months: $
7. Any herbal supplements, homeopathic remedies, and/or nutraceuticals? Yes No
8. Do any of your products include:
   a. Caffeine exceeding 300 mg per servicing (all sources)? Yes No
   b. Cannabidiol (CBD) hemp products? Yes No
   c. Class I & Class II Medical Products / Devices? Yes No
9. Do you mix or compound any ingredients? Yes No
10. Is a prescription required for any of the products you sell? Yes No
11. Are products of others sold or re-packaged under your label? Yes No
12. Do all of your labels include a disclaimer that the FDA has not evaluated the claims on your labels and that your products are not intended to diagnose, treat, cure or prevent any diseases? Yes No
13. Do you obtain Certificates of Insurance from all suppliers evidencing Product Liability Insurance? Yes No
14. Are foreign products sold, distributed, or used as components? Yes No
15. Have any of your products been recalled, discontinued or changed? Yes No
16. Do you offer training or instruction to the user of your products? Yes No

17. Do you offer guarantees, warranties or Hold Harmless agreements with your products? Yes No
18. Do you install, service of demonstrate products? Yes No
19. Is research and development conducted or new products? Yes No

SECTION IV – CLAIMS

PROVIDE 5 YEARS OF CURRENTLY VALUED LOSS RUNS.

20. Has any general liability claim or suit been brought against you and/or any of your employees? Yes No
    If Yes, complete a Supplemental Claim Information Form for each and every claim or suit.
21. Are any persons or entities proposed for this insurance aware of any fact, circumstance, or situation which may result in a GL claim, and has not been reported to your current GL insurance carrier? None to Report Yes No
    If Yes, provide details:
22. Are you aware of any incident, condition, circumstance, defect or suspected defect in any product, which may result in a claim or claims against you that are not listed above? None to Report Yes No
    If Yes, provide details:

NOTICE TO APPLICANT: By signing this application, you agree the answers you give us in this application and any other information you give us as part of the application process are:

1. **Accurate & Complete.**
2. **Given to us to issue you an insurance policy.**
3. **Material to our decision-making process in issuing you an insurance policy.**
4. **A significant part of what we relied upon in making our decision in issuing you an insurance policy. You must agree to notify us, through your insurance brokerage, if during the policy term any material changes to your operations occur.**

Fraud Notices

Applicable in AL, AR, DC, LA, MD, NM, RI and WV: 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. *Applies in MD only.

Applicable in CO: It is unlawful to knowingly provide false, incomplete, or misleading facts or information to an insurance company for the purpose of defrauding or attempting to defraud the company. Penalties may include imprisonment, fines, denial of insurance and civil damages. Any insurance company or agent of an insurance company who knowingly provides false, incomplete or misleading facts or information to a policyholder or claimant for the purpose of defrauding or attempting to defraud the policyholder or claimant with regard to a settlement or award payable from insurance proceeds shall be reported to the Colorado Division of Insurance within the Department of Regulatory Agencies.

Applicable in FL and OK: 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)*. * Applies in FL only.

Applicable in KS: Any person who knowingly and with intent to defraud, presents, causes to be presented, or prepares with knowledge or belief that it will be presented, to or by an insurer, purported insurer, broker or any agent thereof, any written statement as part of, or in support of, an application for the issuance of, or the rating of an insurance policy for personal or commercial insurance, or a claim for payment or other benefit pursuant to an insurance policy 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.

Applicable in KY, NY, OH and PA: 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 (not to exceed five thousand dollars and the stated value of the claim for each such violation)*. *Applies in NY only.

Applicable in ME, TN, VA, and WA: 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 and denial of insurance benefits. *Applies in ME only.

Applicable in NJ: Any person who includes any false or misleading information on an application for an insurance policy is subject to criminal and civil penalties.

Applicable in OR: Any person who knowingly and with intent to defraud or solicit another to defraud the insurer by submitting an application containing a false statement as to any material fact may be violating state law.

Applicable in PR: Any person who knowingly and with the intention of defrauding presents false information in an insurance application, or presents, helps, or causes the presentation of a fraudulent claim for the payment of a loss or any other benefit, or presents more than one claim for the same damage or loss, shall incur a felony and, upon conviction, shall be sanctioned for each violation by a fine of not less than five thousand dollars ($5,000) and not more than ten thousand dollars ($10,000), or a fixed term of imprisonment for three (3) years, or both penalties. Should aggravating circumstances [be] present, the penalty thus established may be increased to a maximum of five (5) years, if extenuating circumstances are present, it may be reduced to a minimum of two (2) years.

Applicable in all other States: 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 material fact, commits a fraudulent insurance act, which is a crime and may also be subject to civil penalty.

Other State Notices

Applicable in RI: THIS INSURANCE CONTRACT HAS BEEN PLACED WITH AN INSURER NOT LICENSED TO DO BUSINESS IN THE STATE OF RHODE ISLAND BUT APPROVED AS A SURPLUS LINES INSURER. THE INSURER IS NOT A MEMBER OF THE RHODE ISLAND INSURERS INSOLVENCY FUND. SHOULD THE INSURER BECOME INSOLVENT, THE PROTECTION AND BENEFITS OF THE RHODE ISLAND INSURERS INSOLVENCY FUND ARE NOT AVAILABLE.

I/We understand that this is an application for insurance only and that the completion and submission of this Application does not bind the Company to sell nor the applicant to purchase this insurance. I/We hereby declare that the above statements and particulars are true and I/we agree that this Application shall be the basis for any contract of insurance issued by the Company in response to it.

Electronic Signature of Applicant or Authorized Representative:

Title: Date:

If you prefer not to return the questionnaire with an electronic signature, please print and sign.