KaMMCO
Kansas Medical Mutual Insurance Company

623 S.W. 10th Avenue
Topeka, Kansas 66612
800-232-2259 | 785-232-2224
www.KaMMCO.com

Cyber Security Insurance for Facilities

NOTICE: THIS APPLICATION IS FOR CLAIMS-MADE AND REPORTED INSURANCE. THE COVERAGE PROVIDES THAT THE LIMIT OF LIABILITY AVAILABLE TO PAY JUDGMENTS, SETTLEMENTS OR ANY OTHER LOSS WILL BE REDUCED AND MAY BE COMPLETELY EXHAUSTED BY DEFENSE COSTS. DEFENSE COSTS WILL BE APPLIED TO THE RETENTION AMOUNT. READ THE ENTIRE APPLICATION CAREFULLY.

The Insurer agrees to use all information provided in this Application solely in connection with the proposed insurance.

If a material change occurs to any of the answers given below prior to the inception of any insurance, the Applicant must notify the insurer, and at the sole discretion of the insurer, any outstanding quotations may be modified or withdrawn.

The particulars, representations and statements contained in this Application, and any other information submitted, are the basis for the proposed Policy, should a Policy be issued.

The Applicant is required to make internal inquiry before completing this Application. This Application must be completed in type or ink by the Applicant. All questions must be answered for a quotation to be given. If more space is needed, please continue your answers on a separate sheet and attach it to this form.

"You" and "your" as used in this Application shall mean the Applicant.

Please attach a copy of your most recent audited financials with the submission.

The completion and signing of this Application does not bind the Applicant or the insurer to a policy or certificate of insurance.

SECTION I. GENERAL INFORMATION

1. Name of Applicant: _____

   Physical Address: _____

   City: _____ State: _____ Zip: _____

   Telephone Number: _____ Fax Number: _____

   Website: _____

2. Type of Institution:

   ☐ Acute Care Hospital ☐ Teaching Hospital ☐ Community Teaching Hospital ☐ Community Hospital
   ☐ For Profit ☐ Non Profit ☐ Skilled Nursing Facility ☐ Home Health
   ☐ Other (please specify): _____

3. Date established: _____

4. Please provide a list of subsidiaries and entities owned by the Applicant. Please describe the nature of business of each such subsidiary or entity, its relationship to the Applicant, and the percentage of ownership by the Applicant.

   _____

   _____

5. Applicant's Projected Revenue for the next 12 months: $_____

Current Year: $_____

One Year Ago: $_____

SECTION II. NETWORK SECURITY AND PRIVACY CONTROLS

6. Do your privacy and security policies include mandatory training for all employees? ☐ Yes ☐ No

7. Do you enforce privacy and security policies that must be followed by all employees, contractors, or other individuals or organizations with access to your patients' information? ☐ Yes ☐ No

8. Do you have a program in place which ensures compliance with HIPAA? ☐ Yes ☐ No

9. Do you process, store, or handle credit card transactions? ☐ Yes ☐ No

   If you answered "**YES"** to question 9, are you PCI-DSS compliant? ☐ Yes ☐ No

10. Do you collect zip codes from customers at point of sale? ☐ Yes ☐ No

    If you answered "**YES"** to question 10, are you compliant with the Song-Beverly Credit Card Act of 1971? ☐ Yes ☐ No

11. Do you have firewalls, information systems and security mechanisms in place? ☐ Yes ☐ No

    If you answered "**YES"** to question 11, are your firewalls, information systems and security mechanisms securely configured? ☐ Yes ☐ No

    Check "NO" if your systems are configured using factory default settings.

12. Do you enforce a software update process that includes monitoring of vendors or automatically receiving notices from them for availability of security patches, upgrades, testing and installing critical security patches? ☐ Yes ☐ No

    If you answered **"YES"** to question12, how frequently is this done? ☐ Weekly ☐ Within 30 days ☐ More than 30 days

13. Does your virus or malicious code control program address the following: anti-virus on all systems, filtering of all content for malicious code, controls on shared drives and folders, CERT or similar vendor neutral threat notification services, removal of spyware and similar parasitic code? ☐ Yes ☐ No

14. Do you test your security at least yearly to ensure effectiveness of your technical controls as well as your procedures for responding to security incidents (e.g. hacking, viruses, and denial of service attacks)? ☐ Yes ☐ No

    If you answered **"YES"** to question 14, does this include a network penetration test? ☐ Yes ☐ No

15. Is all remote access to your network authenticated and encrypted? ☐ Yes ☐ No

16. Do you require all third parties to whom you entrust sensitive or non-public personal information to contractually agree to protect such information using safeguards at least equivalent to your own? ☐ Yes ☐ No

17. Do you require third parties to indemnify you in the event that they suffer a security/privacy breach? ☐ Yes ☐ No

18. 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 them using a technique that leaves no residual information? ☐ Yes ☐ No

19. Do you employ physical security controls to prevent unauthorized access to computer networks and data? ☐ Yes ☐ No

20. Do you control and track all changes to your network to ensure that it remains secure? ☐ Yes ☐ No

21. How long does it take to restore the Applicant's operations after a computer attack or other loss/corruption of data?

    ☐ 12 hrs or less ☐ 12-24 hrs ☐ More than 24 hrs

22. Is all sensitive and confidential information that is transmitted within and from your organization encrypted using industry-grade mechanisms? ☐ Yes ☐ No

23. Is all sensitive and confidential information stored on your organization's databases, servers and data files encrypted? ☐ Yes ☐ No

24. If encryption is not in place for databases, servers and data files, are the following compensating controls in place:

    a) Segregation of servers that store confidential information? ☐ Yes ☐ No

b) Access control with role-based assignments? ☐ Yes ☐ No

25. If your organization stores personal information on portable devices, including laptops, cell phones, PDA's, back-up Tapes, USB thumb drives and external hard drives, is such data encrypted to industry standards? ☐ Yes ☐ No

If you do not store personal information on portable devices, check here ☐

26. Within the past two (2) years, have you completed an outside privacy audit or have you received a privacy certification? ☐ Yes ☐ No

If you answered "**YES"** to question 26, have all deficiencies been resolved? ☐ Yes ☐ No

If there were no deficiencies or recommendations cited, check here ☐

27. Within the last two (2) years, have you completed an internal audit or assessment to determine compliance with regulations or laws concerning the protection of privacy rights? ☐ Yes ☐ No

If you answered **"YES"** to question 27, have all deficiencies been resolved? ☐ Yes ☐ No

If there were no deficiencies or recommendations cited, check here ☐

28. Please estimate the number of patient/customer and employee records you store either electronically or in paper files: _____

SECTION III. LOSS HISTORY

After internal inquiry, have you or any member of your staff, or any person or entity proposed for this insurance:

29. Been investigated for violations of HIPAA or any other state, local or federal law or regulation concerning the confidentiality, access, control and/or use of private information? ☐ Yes ☐ No

30. Experienced any incidents, or received any complaints or claims, or been the subject in litigation involving matters of privacy injury, identity theft, denial of service attacks, computer virus infections, theft of information, damage to third party networks, or your customer's ability to rely on your network? ☐ Yes ☐ No

31. Been non-renewed, placed on extension or declined for similar insurance? ☐ Yes ☐ No

32. In the last five (5) years, had knowledge of any security breaches, privacy breaches, privacy-related incidents, or allegations of breach of privacy? ☐ Yes ☐ No

If any of your answers to questions 29 through 32 is "YES", please explain on a separate sheet of paper.

SECTION IV. REPRESENTATIONS

1. **The undersigned declares that the statements herein are true and correct and that reasonable efforts have been made to obtain sufficient information to facilitate the proper and accurate completion of this Application. The signing of this Application does not bind the undersigned to complete the insurance.**

2. **It is represented that the particulars and statements contained in this Application and any materials submitted herewith (which shall be retained on file by Underwriters and which shall be deemed the basis for the proposed Policy, should a Policy be issued). Underwriters hereby are authorized to make any investigation and inquiry in connection with this Application as they may deem necessary.**

3. **The undersigned agrees that in the event this Application contains misrepresentations or fails to state facts materially affecting the risk assumed by the insurer, the Policy may be cancelled in accordance with the cancellation provisions of the Policy.**

4. **It is agreed that, if after the date of this Application and prior to issuance of the insurance policy, any information supplied on this Application changes, the undersigned shall immediately notify the insurer of such change(s) and shall provide the insurer with any information that would complete, update or correct the information contained in this Application. Any outstanding quotations may be modified or withdrawn at the sole discretion of the insurer.**

5. **For purposes of creating a binding contract of insurance by this Application or in determining the rights and obligations under such a contract in any court of law, the parties acknowledge that a signature reproduced by either facsimile or photocopy shall have the same force and effect as an original signature and that the original and any such copies shall be deemed one and the same document.**

Severability: No knowledge or information possessed by any insured person will be implied to any other insured person except for material facts or information known to the person or persons who signed the Application. In the event that any of the particulars or statements in the Application are untrue, this policy will be void with respect to any insured person who knew of such untruth or to who such knowledge is implied.

Authorized Signature: _____
(Must be signed by the Applicant's President, CEO or COO and dated no more than 45 days prior to binding coverage)

Title: _____ Print Name: _____

Applicant Organization: _____ Date (MM/DD/YYYY): _____