Endurance

ENDURANCE PREMIER PRIVACY
NETWORK SECURITY & INFORMATION MANAGEMENT APPLICATION

This is an Application for a claims made and reported policy. Please read the entire Application carefully before signing. Please answer all questions and attach all requested materials including the following:

☐ Standard contracts or engagement letters used with vendors and subcontractors
☐ Latest fiscal year end and current interim financial statements for all entities proposed for coverage

APPLICANT INFORMATION

1. Name of Applicant: _____
2. Year Established: _____
3. Business Address: _____
4. City, State, Zip: _____
5. Business Website Addresses: _____
6. Nature of Applicant's Business: _____
7. Number of full time employees: _____
8. Applicant is a: □ Corporation □ LLC □ Partnership □ Other: _____

   a. Is the Applicant owned or controlled by, or affiliated with, any other entity? □ Yes □ No
   b. Has the name of the Applicant ever been changed? □ Yes □ No
   c. Is the Applicant a franchisee or franchisor? □ Yes □ No
   d. Does Applicant have any businesses outside the US and Canada? □ Yes □ No

   If the response to any part of Question 8 is "Yes," please attach complete details.

9. Please provide the total gross revenue for the past fiscal year and for the next 12 months.

Fiscal Year End (Month/Year)	United States Revenue	Foreign Revenue	Total Revenue
_____	$_____	$_____	$_____
_____	$_____	$_____	$_____

10. Please provide the following information for all subsidiaries for which coverage is desired.

Name of Subsidiary	Location	Nature of Business	Applicant's % of Ownership

NETWORK SECURITY ORGANIZATION, TRAINING, AND HR MANAGEMENT

11. Has your organization established enterprise-wide responsibility for data security and records management that rests with a single individual or team? □ Yes □ No

12. Does your organization have a written information security policy? □ Yes □ No

13. Does your organization have a written records and information management policy? □ Yes □ No

    If "Yes," are there formal mechanisms to deal with noncompliance? □ Yes □ No

14. Does your organization have an enterprise-wide privacy policy? □ Yes □ No

    If "Yes," is it publicized on your website or through contracts or click-through agreements? □ Yes □ No

15. Does your organization conduct mandatory information security and privacy training for all employees? □ Yes □ No

16. Are background checks conducted prior to hiring new employees? □ Yes □ No

    If "Yes," do they include a credit check? □ Yes □ No

17. Do the policies and procedures established between your Human Resources and Information Technology departments address both friendly and unfriendly employee terminations? □ Yes □ No

RISK MANAGEMENT

18. Are physical security controls in place to regulate access to network equipment? □ Yes □ No

19. Is firewall technology used at all internet points-of-presence? □ Yes □ No

20. Is remote access technology employed allowing users to securely "tunnel in" to the corporate network? □ Yes □ No

21. Is a formal password management program in place? □ Yes □ No

    If "Yes:," does it require users to employ a certain level of complexity? □ Yes □ No
    If "Yes," does it require users to periodically change their passwords? □ Yes □ No

22. Is antivirus scanning and mitigation technology in place on all desktops, laptops, and servers? □ Yes □ No

    If "Yes," are antivirus applications automatically updated? □ Yes □ No

23. Are enterprise and application software patches consistently applied? □ Yes □ No

24. Are network device (router, bridge, firewall) patches consistently applied? □ Yes □ No

25. Are upgrades tested on non-production systems before being put into production? □ Yes □ No □ N/A

26. Is any intrusion prevention or detection technology currently employed on your organization's network? □ Yes □ No

27. Has a qualified third party tested your organization's security controls within the past twelve months? □ Yes □ No

    If "Yes," have all critical recommendations been implemented? □ Yes □ No
    If critical recommendations have not been implemented please explain: _____
    _____
    _____

28. Do you employ Data Leakage Prevention software? □ Yes □ No

DATA ENCRYPTION

29. Is a formal enterprise-wide encryption policy currently in place? □ Yes □ No

30. Does your organization encrypt:

    -data in transit (within your network and to external parties)? □ Yes □ No
    -data at rest within mainframes and/or servers? □ Yes □ No
    -data residing on portable devices or media? □ Yes □ No
    -data residing on backup media? □ Yes □ No

31. Are internal wireless networks encrypted to a WPA or WPA2 standard? □ Yes □ No

32. Do you employ strong access control requirements for laptops and portable devices? □ Yes □ No

33. Do you employ hard drive encryption for laptops and portable devices? □ Yes □ No

34. Do you employ technology to remotely wipe the memories of laptops and portable devices which have been lost or stolen? □ Yes □ No

PRIVACY CONTROLS

35. What kind of third party data do you store or process, including information gathered from your website(s)? (Check all that apply)

□ Medical Record or Personal Health Information (PHI)
□ Social Security Numbers
□ Financial Data, Bank Records, or Investment Data
□ Credit or Debit Card Information
□ Intellectual Property Assets
□ Other (please describe) _____

36. Does your organization have an information classification program which includes data classification standards (e.g. public information, internal/eyes only, sensitive/confidential)? □ Yes □ No

If "Yes," does the program require more stringent controls over the location, encryption, access and scheduled destruction of this information? □ Yes □ No

37. Does your organization have written procedures in place to protect the personally identifiable information (PII) of customers and employees? □ Yes □ No

38. Do any of the organization's websites or software employ the use of cookies, adware or similar technology for the collection of user information? □ Yes □ No

39. Does your organization sell or share individual subscriber or user identifiable information with other internal or external entities? □ Yes □ No □ N/A

If "Yes," do you obtain consent? □ Yes □ No

40. Please identify all relevant regulatory and industry-supported compliance frameworks applicable to your organization:

□ Gramm-Leach-Bliley Act □ HIPAA
□ FACTA Identity Red Flags □ HITECH
□ PCI □ Other (describe): _____

Is your organization currently compliant with all applicable privacy regulations? □ Yes □ No □ N/A

INCIDENT RESPONSE AND DISASTER RECOVERY PLANNING

41. Are systems and databases backed up on a regular basis? □ Yes □ No

If "Yes," how often? □ Continuously □ Daily □ Weekly □ Other: _____
If "Yes," are backup tapes stored offsite? □ Yes □ No

42. Are data backup and recovery procedures periodically tested? □ Yes □ No

If "Yes," how often? _____

43. Are system logs actively maintained on mission-critical servers and appliances? □ Yes □ No

If "Yes," how long are they kept? _____
If "Yes," how often are they reviewed? _____

44. Does your organization have an information security incident response plan in place for network intrusion and virus incidents? □ Yes □ No

If "Yes," does your security incident response plan include alternative options in the event that critical third party functions are incapacitated? □ Yes □ No

45. Does your organization have a formal disaster recovery and business continuity plan? □ Yes □ No

If "Yes," how often is the plan tested? _____

46. Are system backup and recovery procedures tested for all mission-critical systems? □ Yes □ No

47. Approximately how long would it take to restore operations using current methodology?
□ less than or equal to 12 hours □ between 13 and 24 hours □ 24 hours or longer □ Other: _____

VENDOR MANAGEMENT

48. Does your organization conduct reviews of third party vendors with access to your network or which handle sensitive employee or customer information? □ Yes □ No

If "Yes," are vendors and/or service providers contractually held to industry or regulatory standards? □ Yes □ No

49. Does your organization require vendors and third party service providers to indemnify your organization for network security breaches or privacy events that they cause? □ Yes □ No

If "Yes," are they asked to provide evidence of security and privacy liability insurance coverage? □ Yes □ No

50. Does your organization require vendors to carry security and privacy liability insurance? □ Yes □ No

If "Yes," what is the minimum limit of liability required? _____

51. Does your organization require vendors who may have access to sensitive information to use two factor authentication? □ Yes □ No

MEDIA CONTROLS

52. Does your organization use material provided by third parties, including content, music, graphics or video streams on your websites? □ Yes □ No

If "Yes," are written licenses or consents always obtained prior to display? □ Yes □ No

53. Are procedures in place for the formal legal review of all web content prior to display? □ Yes □ No

54. Are procedures in place to respond to allegations that any content created, displayed or published is libelous, infringing, or in violation of any third party's privacy rights? □ Yes □ No

55. Have all corporate trademarks been legally reviewed and approved prior to first use? □ Yes □ No

56. Within the past five years has the organization received a complaint, injunction or cease and desist order alleging trademark or copyright infringement, defamation or privacy violations? □ Yes □ No

If "Yes," please describe: _____
_____
_____

57. Does your organization have a formal social media policy? □ Yes □ No

If "Yes," are strict guidelines in place to ensure only qualified personnel are permitted to post on social media sites? □ Yes □ No

PRIOR AND CURRENT INSURANCE

58. List all network security and privacy liability insurance carried for each of the past three years.

Insurance Company	Limit	SIR	Premium	Policy Period

59. Retroactive Date on current policy: _____

60. Has the Applicant had any Network Security and Privacy Liability Insurance declined, cancelled or non-renewed within the past three years? □ Yes □ No

If "Yes," please attach complete details.

REQUESTED COVERAGE

61. Effective Date Requested: _____

Coverage Part	Coverage Desired	Limit
Network Security, Privacy Liability and Media Liability	□ Yes □ No	$
Privacy Breach Costs	□ Yes □ No	$
Business Income Loss	□ Yes □ No	$
Contingent Business Income Loss	□ Yes □ No	$
Digital Asset Loss	□ Yes □ No	$
Cyber Extortion Threat	□ Yes □ No	$
PCI Assessments	□ Yes □ No	$

62. Self-Insured Retention Desired (each claim): □ $5,000 □ $10,000 □ $25,000 □ $50,000 □ $100,000 □ Other $ _____

63. Additional coverage requests – Please describe_____

COMPANY EXPERIENCE

64. Have any privacy or network security-related claims, suits or proceedings (including without limitation: any shareholder action or derivative suit; or any civil, criminal, or regulatory action, or any complaint, investigation or proceeding related thereto) been made during the past five years against: (a) the Applicant; (b) its predecessors in business; (c) any subsidiary or affiliate of the Applicant; (d) any other entity proposed for coverage; or (e) any past or present principal, partner, managing member, director, officer, employee, leased employee or independent contractor of the Applicant, its predecessors in business, any subsidiary or affiliate of the Applicant or any other entity proposed for coverage? □ Yes □ No

65. Is the Applicant (after diligent inquiry of each principal, partner, managing member, director or officer) aware of any fact, circumstance, incident, situation, or accident (including without limitation: any shareholder action or derivative suit; or any civil, criminal, or regulatory action, or any complaint, investigation or proceeding related thereto) that may result in a privacy or network security-relate claim being made against: (a) the Applicant; (b) its predecessors in business; (c) any subsidiary or affiliate of the Applicant; (d) any other entity proposed for coverage; or (e) any past or present principal, partner, managing member, director, officer, employee, leased employee or independent contractor of the Applicant, its predecessors in business, any subsidiary or affiliate of the Applicant or any other entity proposed for coverage? □ Yes □ No

If the response to either of the questions in the Company Experience section is "Yes," please attach complete details.

NOTE: It is agreed that any claim or lawsuit against the Applicant, or any principal, partner, managing member, director, officer or employee of the Applicant, or any other proposed insured, arising from any fact, circumstance, act, error or omission disclosed or required to be disclosed in response to Questions 64 or 65, is hereby expressly excluded from coverage under the proposed insurance policy.

66. Has the Applicant reported the matters listed in Questions 64 or 65 to its current or former insurance carrier? □ Yes □ No □ N/A

NOTICE – PLEASE READ CAREFULLY

The undersigned, as authorized agent of all individuals and entities proposed for this insurance, declares that, to the best of his/her knowledge and belief, after diligent inquiry of each principal, partner, managing member, director, officer and employee of the Firm, the statements in this Application, including any Supplements are true and complete and will be relied upon by the Insurer in issuing any policy. The undersigned agrees that if the information provided in this Application, including any Supplements changes between the time this Application, including any Supplements is executed and the time the proposed insurance policy is bound or coverage is commenced, the Applicant will immediately notify the Insurer in writing of such changes, and that the Insurer may withdraw or modify any outstanding quotations or agreements to bind the insurance. The undersigned hereby authorizes the Insurer to make any inquiry in connection with the information, statements and disclosures provided in this Application, including any Supplements and further authorizes the release of claim information from any prior insurer to the Insurer.

The undersigned declares that all individuals and entities proposed for this insurance understand and accept that the policy applied for provides coverage for only those claims that are first made against the Insured and reported in writing to the Insurer during the policy period or any extended reporting period (if applicable) and that the limits of liability contained in the policy will include both Damages and Claim Expenses.

The signing of this Application, including any Supplements does not bind the Insurer to offer nor the undersigned to purchase the insurance, but it is agreed this Application, including any Supplements shall be the basis of the insurance and shall be considered physically attached to and become part of the Policy should a Policy be bound and issued. All attachments and information submitted to or obtained by the Insurer in connection with this Application, including any Supplements are hereby incorporated by reference into this Application and made a part hereof.

FRAUD NOTIFICATION

Arkansas Any person who knowingly presents a false or fraudulent claim for payment of a loss or benefit or knowingly presents false information in an application for insurance is guilty of a crime and may be subject to fines and confinement in prison.

Colorado 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.

District of Columbia WARNING: It is a crime to provide false or misleading information to an insurer for the purpose of defrauding the insurer or any other person. Penalties include imprisonment and/or fines. In addition, an insurer may deny insurance benefits if false information materially related to a claim was provided by the applicant.

Florida Any person who knowingly and with intent to injure, defraud, or deceive any insurance company files a statement of claim containing any false, incomplete, or misleading information is guilty of a felony of the third degree.

Hawaii Presenting a fraudulent claim for payment of a loss or benefit is a crime punishable by fines or imprisonment, or both.

Idaho Any person who knowingly, and with intent to defraud or deceive any insurance company, files a statement containing any false, incomplete or misleading information is guilty of a felony.

Indiana A person who knowingly and with intent to defraud an insurer files a statement of claim containing any false, incomplete, or misleading information commits a felony.

Kentucky Any person who knowingly and with intent to defraud any insurance company or other person files an application for insurance 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.

Louisiana Any person who knowingly presents a false or fraudulent claim for payment of a loss or benefit or knowingly presents false information in an application for insurance is guilty of a crime and may be subject to fines and confinement in prison.

Maine 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 denial of insurance benefits.

Maryland Any person who knowingly and willfully presents a false or fraudulent claim for payment of a loss or benefit or who knowingly and willfully presents false information in an application for insurance is guilty of a crime and may be subject to fines and confinement in prison.

Minnesota A person who files a claim with intent to defraud or helps commit a fraud against an insurer is guilty of a crime.

New Jersey Any person who includes any false or misleading information on an application for an insurance policy is subject to criminal and civil penalties.

New York 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 shall also be subject to a civil penalty not to exceed five thousand dollars and the stated value of the claim for each such violation.

Ohio Any person who, with intent to defraud or knowing that he is facilitating a fraud against an insurer, submits an application or files a claim containing a false or deceptive statement is guilty of insurance fraud.

Oklahoma 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.

Pennsylvania 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.

Rhode Island Any person who knowingly presents a false or fraudulent claim for payment of a loss or benefit or knowingly presents false information in an application for insurance is guilty of a crime and may be subject to fines and confinement in prison.

Tennessee It is a crime to knowingly provide false, incomplete or misleading information to an insurance company for the purpose of defrauding the company. Penalties include imprisonment, fines and denial of insurance benefits.

Virginia It is a crime to knowingly provide false, incomplete or misleading information to an insurance company for the purpose of defrauding the company. Penalties include imprisonment, fines and denial of insurance benefits.

Washington It is a crime to knowingly provide false, incomplete or misleading information to an insurance company for the purpose of defrauding the company. Penalties include imprisonment, fines and denial of insurance benefits.

West Virginia Any person who knowingly presents a false or fraudulent claim for payment of a loss or benefit or knowingly presents false information in an application for insurance is guilty of a crime and may be subject to fines and confinement in prison.

The Application, including any Supplements must be signed and dated by a Principal, Partner, Managing Member or Senior Officer of the Applicant. Electronically reproduced signatures will be treated as original.

_____
Date (Mo./Day/Yr.)

_____
Applicant Signature

_____
Print or Type Name

_____
Title

Endurance

ENDURANCE PCI AND RETAIL SUPPLEMENTAL APPLICATION

Please complete if your organization is subject to Payment Card Industry (PCI) standards.

1. Please identify your organization's PCI Level (1-4): □ 1 □ 2 □ 3 □ 4

   Please approximate the percentage of revenue generated by:
   Card-not-present transactions: _____%
   POS Terminals: _____%

   Number of credit/debit transactions annually: _____
   Average dollar value per transaction: $ _____

2. Has your organization achieved PCI compliance? □ Yes □ No

   If "Yes," have you achieved PCI DSS V3 compliance? □ Yes □ No

3. What was the date of your last PCI DSS assessment? _____

4. What percentage of your most recent PCI audit was identified as adequate or in place? _____ %

5. For any standards identified as inadequate or not in place, what percentage have been remediated since the last audit? _____ %

Please complete if your organization employs point-of-sale (POS) systems

6. Approximately how many POS terminals or electronic cash registers does your organization currently manage? _____

7. Are POS systems segregated from your organization's network? □ Yes □ No

8. Do the POS systems have anti-tampering features? □ Yes □ No

9. Is a POS network segmentation strategy employed to ensure that any systems compromise is limited to a single portion of the POS network? □ Yes □ No

10. Please describe your organization's POS system configuration: _____
    _____
    _____
    _____

    Does it employ point-to-point or end-end-end encryption, including the card swipe? □ Yes □ No
    Does it meet the EMV standard? □ Yes □ No

11. Do you outsource your POS system to a third party? □ Yes □ No

    If "Yes," is the vendor supplying a fully encrypted (P2PE) solution? □ Yes □ No
    If "Yes," how are POS vendors vetted? _____
    _____
    _____

12. If P2PE is in place, to what extent is this technology deployed throughout your POS network?

    □ all sites
    □ some sites with the balance getting full encryption at the next scheduled upgrade

    At what date do you expect your POS network to be fully encrypted? _____

13. Does the organization utilize SSL inspection to monitor what is moving through encrypted channels? □ Yes □ No

14. How often are POS systems and electronic cash registers reviewed for security integrity and tested for malware? _____
_____
_____

15. If your organization has not deployed P2PE, what is being done to protect the POS network from compromise?

Is the network being intentionally segregated? □ Yes □ No
Are system and security log files being reviewed frequently for malware signatures? □ Yes □ No

The Application, **including any Supplements must be signed and dated by a Principal, Partner, Managing Member or Senior Officer of the Applicant. Electronically reproduced signatures will be treated as original.**

_____
Date (Mo./Day/Yr.)

_____
Applicant Signature

_____
Print or Type Name

_____
Title

Endurance

ENDURANCE CLOUD AND THIRD PARTY SERVICE PROVIDER SUPPLEMENTAL APPLICATION

1. Please identify third party vendors providing any of the following services, including the approximate number of customer records in their care:

	Name of Vendor	Approx. # of Customer Records
Internet Service Provider		
Website Hosting		
Co-Location		
Managed Security		
Credit card processing		
Software As A Service (SAAS)		
Infrastructure As A Service (IAAS)		
Platform As A Service (PAAS)		
Other: _____		

2. For each contracted cloud service please provide the following information:

Cloud Provider Name	Type of Cloud (Private, Public, Hybrid)	Approx. # of Customer Records	Encryption In Place?
			□ Yes □ No
			□ Yes □ No
			□ Yes □ No
			□ Yes □ No
			□ Yes □ No
			□ Yes □ No
			□ Yes □ No

3. Who is responsible for the security of the data that resides on each cloud? _____
_____
_____

4. Have you certified that your cloud service providers are compliant with all industry and regulatory standards applicable to your organization? □ Yes □ No

The Application, including any Supplements must be signed and dated by a Principal, Partner, Managing Member or Senior Officer of the Applicant. Electronically reproduced signatures will be treated as original.

_____
Date (Mo./Day/Yr.)

_____
Applicant Signature

_____
Print or Type Name

_____
Title

Endurance

ENDURANCE HEALTHCARE PRIVACY AND SECURITY SUPPLEMENTAL APPLICATION

Please check the applicable blocks that describe your organization:

Healthcare Services Providers

□	Individual Hospital	□	Medical Spa
□	Hospital Network	□	Dentist's Office - Individual
□	University Hospital	□	Dentist's Office - System
□	General practitioner/physician group	□	X-Ray/Imaging Center
□	Specialist	□	Outpatient Facility
□	Clinic	□	Blood Bank/Sperm Bank
□	Home Health Care	□	Other (describe): _____
□	Long Term Care / Hospice Care		

Medical-Related Service Providers

□	Managed Care Organization	□	Records Management Services
□	Insurance Company	□	Billing/Accounting Services
□	Benefits Broker	□	Other Medical-Related Services (describe): _____
□	Healthcare Exchange		

1. For healthcare service providers, please identify the number of facilities in your organization: _____

2. Please list the approximate number of patients treated in the past calendar year: _____

3. Please list the approximate number of Personal Health Information (PHI) records handled in the past calendar year: _____

4. Is your facility associated with a university? □ Yes □ No
   If "Yes," are your systems and network managed independently of the university network? □ Yes □ No

5. Are social security numbers currently used as patient and/or employee identifiers? □ Yes □ No

6. Is your organization HIPAA compliant? □ Yes □ No

7. Please identify the assigned HIPAA Privacy Officer and the number of additional staff working under this individual:
   HIPAA Privacy Officer: _____
   # of additional staff: _____

8. Does your organization have established paper file and Electronic Health Record (EHR) retention and destruction protocols in place? □ Yes □ No
   If "Yes," how long are records currently maintained? _____
   If "Yes," how are these records destroyed? _____
   _____
   _____

9. Please list specific brand names of software used to manage or process your patients' clinical, financial and EHR Information:

_____
_____
_____

10. Has an attorney reviewed the organization's Business Associate Agreements? □ Yes □ No

11. Has the organization updated the Business Associate Agreement to comply with the Omnibus Final Rule of HIPAA? □ Yes □ No

12. Is personal medical information permitted on hospital-provided laptops computers and other handheld devices? □ Yes □ No

13. Does your organization permit employees to use their own smartphones and/or tablets to handle work-related email and documents (e.g. BYOD)? □ Yes □ No

    If "Yes," what technical controls are employed to maintain the security of PHI?

_____
_____
_____

The Application, **including any Supplements must be signed and dated by a Principal, Partner, Managing Member or Senior Officer of the Applicant. Electronically reproduced signatures will be treated as original.**

_____
Date (Mo./Day/Yr.)

_____
Applicant Signature

_____
Print or Type Name

_____
Title