



e-MD® / MEDEFENSE® Plus Insurance Application

THIS IS AN APPLICATION FOR A CLAIMS MADE AND REPORTED POLICY. THIS APPLICATION IS NOT A BINDER.

This application for e-MD® / MEDEFENSE® Plus Insurance is intended to be used for the preliminary evaluation of a submission. When completed in its entirety, this application will enable the Underwriter to decide whether or not to authorize the binding of insurance. Please type or print clearly and answer all questions. If space is insufficient to answer any question fully, attach a separate sheet. Complete all required supplemental forms/applications. "You" and "Your", as used in this application, means the Applicant unless noted otherwise below.

Please refer to the attached Cyber Glossary for an explanation of the cyber security terms that appear in bold face type.

1. GENERAL INFORMATION			
Name of Applicant:			
Street Address:			
City, State, Zip:		Phone:	
Website:		Fax:	
2. FORM OF BUSINESS			
a. Applicant is a(an): <input type="checkbox"/> Individual <input type="checkbox"/> Corporation <input type="checkbox"/> Partnership <input type="checkbox"/> Other: _____			
b. Date established: _____			
c. Description of operations (medical specialty): _____			
d. Current medical professional liability carrier:		Policy number:	
e. Total full-time equivalent physicians: _____			
f. Total number of employees: _____			
g. Attach a list of all subsidiaries, affiliated companies or entities owned by the Applicant and include a description of (1) the nature of operations of each such subsidiary, affiliated company or entity, (2) its relationship to the Applicant and (3) the percentage of ownership by the Applicant.			
3. REVENUES			
	<u>Current</u> Fiscal Year ending / (current projected)	<u>Last</u> Fiscal Year ending /	<u>Two</u> Fiscal Years ago ending /
Total gross revenues:	\$ _____	\$ _____	\$ _____
4. RECORDS (Complete Section 4 only if e-MD (Cyber Liability) coverage is desired.)			
a. Do you collect, store, host, process, control, use or share any private or sensitive information* in either paper or electronic form? If "Yes", provide the approximate number of unique records: Paper records: _____ Electronic records: _____ <small>*Private or sensitive information includes any information or data that can be used to uniquely identify a person, including, but not limited to, social security numbers or other government identification numbers, payment card information, drivers' license numbers, financial account numbers, personal identification numbers (PINs), usernames, passwords, healthcare records and email addresses.</small>			<input type="checkbox"/> Yes <input type="checkbox"/> No
b. Do you collect, store, host, process, control, use or share any biometric information or data, such as fingerprints, voiceprints, facial, hand, iris or retinal scans, DNA, or any other biological, physical or behavioral characteristics that can be used to uniquely identify a person? If "Yes", have you reviewed your policies relating to the collection, storage and destruction of such information or data with a qualified attorney and confirmed compliance with applicable federal, state, local and foreign laws?			<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No
c. Do you process, store or handle credit card transactions? If "Yes", are you PCI-DSS Compliant?			<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No
5. BILLING AND COMPLIANCE (Complete Section 5 only if MEDEFENSE Plus (Regulatory) coverage is desired.)			
a. Your annual projected billings:	\$ _____		
b. Percentage of your annual projected billings attributable to Medicare patients:	% _____		

<p>c. Have you implemented any of the following to protect against phishing messages? (Check all that apply):</p> <p><input type="checkbox"/> Sender Policy Framework (SPF)</p> <p><input type="checkbox"/> DomainKeys Identified Mail (DKIM)</p> <p><input type="checkbox"/> Domain-based Message Authentication, Reporting & Conformance (DMARC)</p> <p><input type="checkbox"/> None of the above</p>	
<p>d. Can your users access email through a web application or a non-corporate device?</p> <p>If "Yes", do you enforce Multi-Factor Authentication (MFA)?</p>	<p><input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>
<p>e. Do you use Office 365 in your organization?</p> <p>If "Yes", do you use the Office 365 Advanced Threat Protection add-on?</p>	<p><input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>
<p>ADDITIONAL COMMENTS (Use this space to explain any "No" answers in the above section and/or to list other relevant IT security measures you are utilizing that are not listed here.)</p>	
<p>8. INTERNAL SECURITY CONTROLS (Complete Section 8 only if e-MD (Cyber Liability) coverage is desired.)</p>	
<p><i>If the answer to any question in this section is "No", please provide additional details in the "Additional Comments" section.</i></p>	
a. Are you HIPAA compliant?	<input type="checkbox"/> Yes <input type="checkbox"/> No
<p>b. Do you use a cloud provider to store data or host applications?</p> <p>If "Yes", provide the name of the cloud provider: _____</p> <p>If you use more than one cloud provider to store data, specify the cloud provider storing the largest quantity of sensitive customer and/or employee records (e.g., including medical records, personal health information, social security numbers, bank account details and credit card numbers) for you.</p>	<input type="checkbox"/> Yes <input type="checkbox"/> No
c. Do you use MFA to secure all cloud provider services that you utilize (e.g. Amazon Web Services (AWS), Microsoft Azure, Google Cloud)?	<input type="checkbox"/> Yes <input type="checkbox"/> No
<p>d. Do you encrypt all sensitive and confidential information stored on your organization's systems and networks?</p> <p>If "No", are the following compensating controls in place:</p> <p>(1) Segregation of servers that store sensitive and confidential information?</p> <p>(2) Access control with role-based assignments?</p>	<p><input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>
<p>e. Do you allow remote access to your network?</p> <p>If "Yes", do you use MFA to secure all remote access to your network, including any remote desktop protocol (RDP) connections?</p> <p>If MFA is used, complete the following:</p> <p>(1) Select your MFA provider: Choose an item.</p> <p>If "Other", provide the name of your MFA provider: _____</p> <p>(2) Select your MFA type: Choose an item.</p> <p>If "Other", describe your MFA type: _____</p> <p>(3) Does your MFA configuration ensure that the compromise of a single device will only compromise a single authenticator?</p>	<p><input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>
<p>f. Do you use a next-generation antivirus (NGAV) product to protect all endpoints across your enterprise?</p> <p>If "Yes", complete the following:</p> <p>(1) Select your NGAV provider: Choose an item.</p> <p>If "Other", provide the name of your NGAV provider: _____</p> <p>(2) Do you enforce application whitelisting/blacklisting?</p> <p>(3) Is an endpoint detection and response (EDR) tool deployed on 100% of endpoints?</p> <p>If "No", use the Additional Comments section to outline which assets do not have EDR, and whether any mitigating safeguards are in place for such assets.</p> <p>(4) Can users access the network with their own device ("Bring Your Own Device")?</p> <p>If "Yes", is EDR required to be installed on these devices?</p>	<p><input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>

ADDITIONAL COMMENTS (Use this space to explain any “No” answers in the above section and/or to list other relevant IT security measures you are utilizing that are not listed here.)

9. BACKUP AND RECOVERY POLICIES (Complete Section 9 only if e-MD (Cyber Liability) coverage is desired.)

If the answer to the question in this section is “No”, please provide additional details in the “Additional Comments” section.

Do you use a data backup solution?

☐ Yes ☐ No

If “Yes”:

a. Which best describes your data backup solution?

☐ Backups are kept locally but separate from your network (**offline/air-gapped backup solution**).

☐ Backups are kept in a dedicated cloud backup service.

☐ You use a cloud-syncing service (e.g. Dropbox, OneDrive, SharePoint, Google Drive).

☐ Other (describe your data backup solution): _____

b. Check all that apply:

☐ Your backups are encrypted.

☐ You have **immutable backups**.

☐ Your backups are secured with different access credentials from other administrator credentials.

☐ You utilize **MFA** for both internal and external access to your backups.

☐ You have tested the successful restoration and recovery of key server configurations and data from backups in the last 6 months.

☐ You are able to test the integrity of backups prior to restoration to ensure that they are free of malware.

c. How frequently are backups run? ☐ Daily ☐ Weekly ☐ Monthly

d. Estimated amount of time it will take to restore essential functions using backups in the event of a widespread malware or ransomware attack within your network?

☐ 0-24 hours ☐ 1-3 days ☐ 4-6 days ☐ 1 week or longer

ADDITIONAL COMMENTS (Use this space to explain any “No” answers in the above section and/or to list other relevant IT security measures you are utilizing that are not listed here.)

10. PHISHING CONTROLS (Complete Section 10 only if e-MD (Cyber Liability) coverage is desired.)

a. Do any of the following employees at your company complete social engineering training:

(1) Employees with financial or accounting responsibilities?

☐ Yes ☐ No

(2) Employees without financial or accounting responsibilities?

☐ Yes ☐ No

If “Yes” to question 10.a.(1) or 10.a.(2) above, does your social engineering training include phishing simulation?

☐ Yes ☐ No

b. Does your organization send and/or receive wire transfers?

☐ Yes ☐ No

If “Yes”, does your wire transfer authorization process include the following:

(1) A wire request documentation form?

☐ Yes ☐ No

(2) A protocol for obtaining proper written authorization for wire transfers?

☐ Yes ☐ No

(3) A separation of authority protocol?

☐ Yes ☐ No

(4) A protocol for confirming all payment or funds transfer instructions/requests from a new vendor, client or customer via direct call to that vendor, client or customer using only the telephone number provided by the vendor, client or customer before the payment or funds transfer instruction/request was received?

☐ Yes ☐ No

(5) A protocol for confirming any vendor, client or customer account information change requests (including requests to change bank account numbers, contact information or mailing addresses) via direct call to that vendor, client or customer using only the telephone number provided by the vendor, client or customer before the change request was received?

☐ Yes ☐ No

11. REGULATORY LOSS HISTORY (Complete Section 11 only if MEDEFENSE Plus (Regulatory) coverage is desired.)

If the answer to any question in 11.a. through 11.b. below is "Yes", please complete a Claim Supplemental Form for each claim, allegation or incident.

a. After internal inquiry, have you, any member of your staff, any other person or entity proposed for this insurance, any consultant, or any person or entity for whom you perform billing services:

(1) Had to refund amounts to government (public) and/or commercial (private) payers within the past three years?

☐ Yes ☐ No

If "Yes", provide estimated amounts:

Current Year (Fiscal): Public: \$ _____ Private: \$ _____

Last Year (Fiscal): Public: \$ _____ Private: \$ _____

Two Years Ago (Fiscal): Public: \$ _____ Private: \$ _____

If "Yes", were these refunds due to an audit, allegation of improper billing or voluntary self-disclosure?

☐ Yes ☐ No

(2) Been placed on prepayment review by any local, state or federal government agency or by any commercial payer?

☐ Yes ☐ No

(3) Been audited, investigated or sanctioned by a local, state or federal government agency or commercial payer regarding Medicare/Medicaid billing practices, utilization of Medicare/Medicaid services or the delivery of health care services or reimbursement thereof?

☐ Yes ☐ No

(4) Been sued or desecrated by a commercial payer?

☐ Yes ☐ No

(5) Been reviewed, investigated or sanctioned by a state medical licensing board?

☐ Yes ☐ No

(6) Been investigated for HIPAA, EMTALA or Stark/anti-kickback violations?

☐ Yes ☐ No

b. Do you or any other person or organization proposed for this insurance have knowledge of any facts, circumstances, situations, events or incidents that could result in a medical regulatory action, regulatory investigation or demand for restitution?

☐ Yes ☐ No

12. CYBER/PRIVACY LOSS HISTORY (Complete Section 12 only if e-MD (Cyber Liability) coverage is desired.)

If the answer to any question in 12.a. through 12.c. below is "Yes", please complete a Claim Supplemental Form for each claim, allegation or incident.

a. In the past 3 years, has the Applicant or any other person or organization proposed for this insurance:

(1) Received any complaints or written demands or been a subject in litigation involving matters of privacy injury, breach of private information, network security, defamation, content infringement, identity theft, denial of service attacks, computer virus infections, theft of information, damage to third party networks or the ability of third parties to rely on the Applicant's network?

☐ Yes ☐ No

(2) Been the subject of any government action, investigation or other proceedings regarding any alleged violation of privacy law or regulation?

☐ Yes ☐ No

(3) Notified customers, clients or any third party of any security breach or privacy breach?

☐ Yes ☐ No

(4) Received any cyber extortion demand or threat?

☐ Yes ☐ No

(5) Sustained any unscheduled network outage or interruption for any reason?

☐ Yes ☐ No

(6) Sustained any property damage or business interruption losses as a result of a cyber-attack?

☐ Yes ☐ No

(7) Sustained any losses due to wire transfer fraud, telecommunications fraud or phishing fraud?

☐ Yes ☐ No

b. Do you or any other person or organization proposed for this insurance have knowledge of any security breach, privacy breach, privacy-related event or incident or allegations of breach of privacy that may give rise to a claim?

☐ Yes ☐ No

c. In the past 3 years, has any service provider with access to the Applicant's network or computer system(s) sustained an unscheduled network outage or interruption lasting longer than 4 hours?

☐ Yes ☐ No

If "Yes", did the Applicant experience an interruption in business as a result of such outage or interruption?

☐ Yes ☐ No

NOTICE TO APPLICANT

The insurance for which you are applying will not respond to incidents about which any person proposed for coverage had knowledge prior to the effective date of the policy nor will coverage apply to any claim or circumstance identified or that should have been identified in questions 11.a. through 12.c. of this application.

NOTICE TO NEW YORK APPLICANTS: ANY PERSON WHO KNOWINGLY AND WITH INTENT TO DEFRAUD ANY INSURANCE COMPANY OR OTHER PERSON FILES AN APPLICATION FOR INSURANCE CONTAINING ANY FALSE INFORMATION, OR CONCEALS FOR THE PURPOSE OF MISLEADING, INFORMATION CONCERNING ANY FACT MATERIAL THERETO, COMMITS A FRAUDULENT INSURANCE ACT, WHICH IS A CRIME.

The Applicant hereby acknowledges that he/she/it is aware that the limit of liability shall be reduced, and may be completely exhausted, by claim expenses and, in such event, the Insurer shall not be liable for claim expenses or any judgment or settlement that exceed the limit of liability.

I HEREBY DECLARE that, after inquiry, the above statements and particulars are true and I have not suppressed or misstated any material fact, and that I agree that this application shall be the basis of the contract with the Underwriters.

CERTIFICATION AND SIGNATURE

The Applicant has read the foregoing and understands that completion of this application does not bind the Underwriter or the Broker to provide coverage. It is agreed, however, that this application is complete and correct to the best of the Applicant's knowledge and belief, and that all particulars which may have a bearing upon acceptability as an e-MD® / MEDEFENSE® Plus Insurance risk have been revealed.

It is understood that this application shall form the basis of the contract should the Underwriter approve coverage, and should the Applicant be satisfied with the Underwriter's quotation. It is further agreed that, if in the time between submission of this application and the requested date for coverage to be effective, the Applicant becomes aware of any information which would change the answers furnished in response to any question of this application, such information shall be revealed immediately in writing to the Underwriter.

This application shall be deemed attached to and form a part of the Policy should coverage be bound.

Must be signed by an officer of the company.

Print or Type Applicant's Name	Title of Applicant
Signature of Applicant	Date Signed by Applicant

California Fraud Warning

For your protection, California law requires the following to appear on this form: Any person who knowingly presents false or fraudulent information to obtain or amend insurance coverage or to make a claim for the payment of a loss is guilty of a crime and may be subject to fines and confinement in state prison.

The following Cyber Glossary is provided to assist you in completing your application correctly and completely.

DomainKeys Identified Mail (DKIM) is an email authentication method that allows senders to associate a domain name with an email message, thus vouching for its authenticity. A sender creates the DKIM by “signing” the email with a digital signature. This “signature” is located in the message's header.

Domain-based Message Authentication, Reporting & Conformance (DMARC) is an email authentication protocol that uses Sender Policy Framework (SPF) and DKIM to determine the authenticity of an email message.

Endpoint application isolation and containment technology is a form of zero-trust endpoint security. Instead of detecting or reacting to threats, it enforces controls that block and restrain harmful actions to prevent compromise. Application containment is used to block harmful file and memory actions to other apps and the endpoint. Application isolation is used to prevent other endpoint processes from altering or stealing from an isolated app or resources.

Common Providers: Authentic8 Silo; BitDefender™ Browser Isolation; CylancePROTECT; Menlo Security Isolation Platform; Symantec Web Security Service

Endpoint Detection and Response (EDR), also known as endpoint *threat* detection and response, centrally collects and analyzes comprehensive endpoint data across your entire organization to provide a full picture of potential threats.

Common Providers: Carbon Black Cloud; Crowdstrike Falcon Insight; SentinelOne; Windows Defender Endpoint

Immutable backups are backup files that are fixed, unchangeable, and can be deployed to production servers immediately in case of ransomware attacks or other data loss.

Multi-Factor Authentication (MFA) is an electronic authentication method in which a computer user is granted access to a website or application only after successfully presenting two or more pieces of evidence to an authentication mechanism: knowledge (e.g., password), possession (e.g., phone or key), and inherence (e.g., FaceID or hand print). MFA for remote email access can be enabled through most email providers.

Common MFA providers for remote network access:

Okta; Duo; LastPass; OneLogin; and Auth0.

Next-Generation Anti-Virus (NGAV) is software that uses predictive analytics driven by machine learning and artificial intelligence and combines with threat intelligence to detect and prevent malware and fileless non-malware attacks, identify malicious behavior, and respond to new and emerging threats that previously went undetected. For purposes of completing this application, NGAV refers to anti-virus protection that focuses on detecting and preventing malware on each individual endpoint. If your organization has a NGAV solution **AND** you are centrally monitoring and analyzing all endpoint activity, please indicate that you have NGAV & EDR on the application.

Common Providers: BitDefender™; Carbon Black; CrowdStrike Falcon Prevent; SentinelOne; Sophos; Symantec

Offline/Air-gapped backup solution refers to a backup and recovery solution in which one copy of your organization's data is offline (i.e., disconnected) and cannot be accessed. If a file or system of files has no connection to the internet or a LAN, it can't be remotely hacked or corrupted.

Powershell is a cross-platform task automation and configuration management framework from Microsoft, consisting of a command-line shell and scripting language. It is used by IT departments to run tasks on multiple computers in an efficient manner. For example, Powershell can be used to install a new application across your organization.

Privileged Account Management Software (PAM) is software that allows you to secure your privileged credentials in a centralized, secure vault (i.e., a password safe). To qualify as PAM, a product must allow administrators to create privileged access accounts; offer a secure vault to store privileged credentials; and monitor and log user actions while using privileged accounts.

Common Providers: CyberArk and BeyondTrust.

Protective DNS Service (PDNS) refers to a service that provides Domain Name Service (DNS) protection (also known as DNS filtering) by blacklisting dangerous sites and filtering out unwanted content. It can also help to detect & prevent malware that uses DNS tunneling to communicate with a command and control server.

Common Providers: Zscaler; Quad9; OpenDNS; and public sector PDNS.

Remote Desktop Protocol (RDP) connections is a proprietary protocol developed by Microsoft which provides a user with a graphical interface to connect to another computer over a network connection. The Microsoft RDP provides remote display and input capabilities over network connections for Windows-based applications running on a server.

Security Information and Event Management system (SIEM) is a subsection within the field of computer security, wherein software products and services combine security information management and security event management. SIEM provides real-time analysis of security alerts generated by applications and network hardware.



Security Operations Center (SOC) is a centralized unit that deals with security issues on an organizational and technical level.

Sender Policy Framework (SPF) is an email authentication technique used to prevent spammers from sending messages on behalf of your domain. With SPF, your organization can publish authorized mail servers.

Vulnerability management tool is a cloud service that gives you instantaneous, global visibility into where your IT systems might be vulnerable to the latest internet threats and how to protect against them. The tool is an ongoing process that includes proactive asset discovery, continuous monitoring, mitigation, remediation and defense tactics to protect your organization's modern IT attack surface from cyber threats.

Common Providers: Qualys; InsightVM by Rapid7; and Nessus® by Tenable™