Cyber & Professional Lines Group
16501 Ventura Blvd. Suite 200, Encino, CA 91436
main (818) 382-2030

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.

1. GENERAL INFORMATION

Name of Applicant:			
Street Address:			
City, State, Zip:		Phone:	
Website:		Fax:	

2. FORM OF BUSINESS

a. Applicant is a(an): ☐ Individual ☐ Corporation ☐ Partnership ☐ 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. Please attach a list of all subsidiaries, affiliated companies or entities owned by the Applicant. Please describe (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

	Current Fiscal Year ending / (current projected)	**Last** Fiscal Year ending /	**Two** Fiscal Years ago ending /
Total gross revenues:	$	$	$

4. RECORDS (Please 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? ☐ Yes ☐ No

If "Yes", please provide the approximate number of unique records:

Paper records: ______________________ **Electronic records:** ______________________

***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.**

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? ☐ Yes ☐ No

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? ☐ Yes ☐ No

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

If "Yes", are you PCI-DSS Compliant? ☐ Yes ☐ No

5. BILLING AND COMPLIANCE (Please 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:	%
c. Percentage of your annual projected billings attributable to Medicaid patients:	%

d. What have your Medicare / Medicaid billings been for each of the past three years:
Current Year: ________________ One Year Ago: ________________ Two Years Ago: ________________________

e. Do you have a billing compliance program in place? □ Yes □ No

If "Yes", when was it implemented? ___________________________

If "No", do you outsource your billings to a third-party billing company? □ Yes □ No

f. Do you use credentialed staff to perform billing procedures? □ Yes □ No

If Yes", how many credentialed staff members do you employ for this purpose? _________________

g. Do you bill all services under the National Provider Identifier (NPI) of the individual who performed the service? □ Yes □ No

If "No', in instances where a mid-level provider's services are billed under a physician's NPI, is that physician present when the services are being rendered? □ Yes □ No

h. Is your practice using a current edition of the CPT manual? □ Yes □ No

i. Is software used to ensure billing compliance? □ Yes □ No

If "Yes", when was the software installed? ____________________________

j. Who within your organization is responsible for billing compliance? Please include the person's name, title, qualifications, date of hire in this position and how often such person performs billing compliance reviews **(use additional sheets if necessary)**.

____

____

6. IT DEPARTMENT (Please complete Section 6 only if e-MD (Cyber Liability) coverage is desired.)

This section must be completed by the individual responsible for the Applicant's network security. As used in this section only, "you" refers to the individual responsible for the Applicant's network security.

a. Who is responsible for the Applicant's network security?

Name:			
Title:			
Phone:		Email address:	
IT Security Designation(s):			

b. The Applicant's network security is: □ Outsourced □ Managed internally/in-house

c. How many IT personnel are on your team?	
d. How many dedicated IT security personnel are on your team?	

By signing below, you confirm that you have reviewed all questions in Sections 7 through 9 of this application regarding the Applicant's security controls, and, to the best of your knowledge, all answers are complete and accurate. Additionally, you consent to receiving direct communications from the Insurer and/or its representatives regarding potentially urgent security issues identified in relation to the Applicant's organization.

Print/Type Name: ______________________________

Signature: ______________________________

7. EMAIL SECURITY CONTROLS (Please complete Section 7 only if e-MD (Cyber Liability) coverage is desired.)

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

a. Do you tag external emails to alert employees that the message originated from outside the organization? □ Yes □ No

b. Do you pre-screen emails for potentially malicious attachments and links? □ Yes □ No

If "Yes", do you have the capability to automatically detonate and evaluate attachments in a sandbox to determine if they are malicious prior to delivery to the end-user? □ Yes □ No

c. Have you implemented any of the following to protect against phishing messages? (*Please check all that apply*):

□ Sender Policy Framework (SPF)
□ DomainKeys Identified Mail (DKIM)
□ Domain-based Message Authentication, Reporting & Conformance (DMARC)
□ None of the above

d. Can your users access email through a web application or a non-corporate device? □ Yes □ No

If "Yes", do you enforce Multi-Factor Authentication (MFA)? □ Yes □ No

e. Do you use Office 365 in your organization? □ Yes □ No

If "Yes", do you use the Office 365 Advanced Threat Protection add-on? □ Yes □ No

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.*)

8. INTERNAL SECURITY CONTROLS (Please complete Section 8 only if e-MD (Cyber Liability) coverage is desired.)

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

a.	Are you HIPAA compliant?	□ Yes □ No
b.	Do you use a cloud provider to store data or host applications? **If "Yes", please provide the name of the cloud provider: ____________________________________** **If you use more than one cloud provider to store data, please 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.**	□ Yes □ 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)?	□ Yes □ No
d.	Do you encrypt all sensitive and confidential information stored on your organization's systems and networks? **If "No", are the following compensating controls in place:** **(1) Segregation of servers that store sensitive and confidential information?** **(2) Access control with role-based assignments?**	□ Yes □ No □ Yes □ No □ Yes □ No
e.	Do you allow remote access to your network? **If "Yes":** **(1) Do you use MFA to secure all remote access to your network, including any remote desktop protocol (RDP) connections?** **If MFA is used, please select your MFA provider:** **If "Other", please provide the name of your MFA provider: ________________________________**	□ Yes □ No □ Yes □ No
f.	Do you use a next-generation antivirus (NGAV) product to protect all endpoints across your enterprise? **If "Yes", please select your NGAV provider:** **If "Other", please provide the name of your NGAV provider: ____________________**	□ Yes □ No
g.	Do you use an endpoint detection and response (EDR) tool that includes centralized monitoring and logging of all endpoint activity across your enterprise? **If "Yes", please select your EDR provider:** **If "Other", please provide the name of your EDR provider: ____________________**	□ Yes □ No
h.	Do you use MFA to protect access to privileged user accounts?	□ Yes □ No
i.	Do you manage privileged accounts using privileged account management software (e.g., CyberArk, BeyondTrust, etc.)? **If "Yes", please provide the name of your provider: ____________________**	□ Yes □ No
j.	Do you actively monitor all administrator access for unusual behavior patterns? **If "Yes", please provide the name of your monitoring tool: ____________________**	□ Yes □ No
k.	Do you roll out a hardened baseline configuration across servers, laptops, desktops and managed mobile devices?	□ Yes □ No
l.	Do you record and track all software and hardware assets deployed across your organization? **If "Yes", please provide the name of the tool used for this purpose (if any): ____________________**	□ Yes □ No
m.	Do non-IT users have local administration rights on their laptop / desktop?	□ Yes □ No
n.	How frequently do you install critical and high severity patches across your enterprise? □ 1-3 days □ 4-7 days □ 8-30 days □ One month or longer	
o.	Do you have any end of life or end of support software? **If "Yes", is it segregated from the rest of your network?**	□ Yes □ No □ Yes □ No
p.	Do you use a protective DNS service (e.g. ZScaler, Quad9, OpenDNS or the public sector PDNS) to block access to known malicious websites?	□ Yes □ No

If “Yes”, please provide the name of your DNS provider: ____________________	
q. Do you use endpoint application isolation and containment technology on all endpoints? **If “Yes”, please select your provider:** **If “Other”, please provide the name of your provider:** ____________________	□ Yes □ No
r. Can users run Microsoft Office Macro enabled documents on their system by default?	□ Yes □ No
s. Do you implement PowerShell best practices as outlined in the [Environment Recommendations by Microsoft]?	□ Yes □ No
t. Do you utilize a Security Information and Event Management (SIEM) system?	□ Yes □ No
u. Do you utilize a Security Operations Center (SOC)? **If “Yes”, is it monitored 24 hours a day, 7 days a week?**	□ Yes □ No □ Yes □ No
v. Do you use a vulnerability management tool? **If “Yes”, please select your provider:** **If “Other”, please provide the name of your provider:** ____________________	□ Yes □ No

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 (Please 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. How frequently does it run? □ **Daily** □ **Weekly** □ **Monthly**	
b. Estimated amount of time it will take to restore essential functions 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**	
c. Please check all that apply: □ **Backups are encrypted.** □ **Backups are kept separate from your network (offline/air-gapped), or in a cloud service designed for this purpose.** □ **Backups are secured with different access credentials from other administrator credentials.** □ **You utilize MFA to restrict access to your backups.** □ **You use a cloud-syncing service (e.g. Dropbox, OneDrive, SharePoint, Google Drive) for backups.** □ **Your cloud-syncing service is protected by MFA.** □ **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.**	

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 (Please 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 <u>before</u> 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 <u>before</u> the change request was received?	□ Yes □ No
11. REGULATORY LOSS HISTORY (Please 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”, please 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 deselected 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 (Please 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

TOKIO MARINE HCC

Cyber & Professional Lines Group

Cyber Glossary

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

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.

Cyber Glossary

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™