

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.

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:											
Stre	et Ac	ddress:									
City, State, Zip: Phone:											
Website: Fax:											
2.	FO	RM OF BUSINESS									
	a.	Applicant is a(an):	☐ Ir	ndividual [☐ Corpora	tion 🔲 P	artnership [Other:			-
	b.	Date established:									
	c.	Description of operation	ns (med	dical specialty):							
	d.	Current medical profes	ssional li	iability carrier:				Policy n	umber:		
	e.	Total full-time equivale	nt physi	icians:						•	
	f.	Total number of emplo	yees:								
	g.	Attach a list of all subs	idiaries,	affiliated comp	anies or e	ntities owne	ed by the Applic	cant and	include a	a description	of (1) the nature
		of operations of each s		osidiary, affiliate	ed compar	ny or entity,	(2) its relations	ship to the	e Applica	ant and (3) t	the percentage of
3.		ownership by the Appl VENUES	icani.								
J.	NE	VENUES		Current Fiscal Y	ear	la	st Fiscal Year			Two Fiscal `	Years ago
			=	ending /	ou.		ending /		=	ending	/
			(current projecte	ed)		Ü			Ū	
Tot	al gr	oss revenues:	\$	-		\$			\$		
Tot		coss revenues:		only if e-MD (Cyber Lia		erage is desire	ed.)	\$		
			ection 4	-	•	bility) cove	-	•		ither paper	☐ Yes ☐ No
	RE	CORDS (Complete Se	ection 4 host, pr	ocess, control,	use or sha	bility) cove	-	•		ither paper	☐ Yes ☐ No
	RE	Do you collect, store, or electronic form?	host, pr	rocess, control,	use or sha	bility) cove are any prive	ate or sensitive	•		ither paper	☐ Yes ☐ No
	RE	Do you collect, store, or electronic form? If "Yes", provide the a Paper records: *Private or sensitive in	host, prapproxim	nate number of	use or sha unique rea Electronia informatior	bility) coverage any privilence ords: cords: corecords: n or data that	ate or sensitive	informat	ion* in e	y a person,	☐ Yes ☐ No
	RE	Do you collect, store, or electronic form? If "Yes", provide the a Paper records: *Private or sensitive in including, but not limit	host, prapproxim	nate number of includes any ocial security nu	use or sha unique rea Electronia information umbers or	bility) coverage any privilence ords: cords: corecords: n or data the other gover	ate or sensitive	to unique	ion* in e	y a person, yment card	☐ Yes ☐ No
	RE	Do you collect, store, or electronic form? If "Yes", provide the a Paper records: *Private or sensitive in	host, prapproxim	nate number of on includes any ocial security numbers, finan	use or sha unique red Electronio information umbers or icial accou	bility) coverage any privilence any privilence any privilence and a cords: and a cords: and a cord a cor	ate or sensitive	to unique	ion* in e	y a person, yment card	☐ Yes ☐ No
	RE	CORDS (Complete Second Property Complete Secon	host, prapproximation formation ded to, so license s, healther, host,	nate number of nincludes any ocial security numbers, financare records and process, conti	use or sha unique rec Electronic informatior umbers or icial accou d email add rol, use o	bility) coverage any privious cords: cords: corecords: n or data that other gover unt number dresses. or share an	at can be used nment identificas, personal ide	to unique ation num entification	ion* in e	y a person, yment card ers (PINs),	☐ Yes ☐ No
	RE	CORDS (Complete Second Property Complete Secon	host, prapproximation formation ded to, so license s, healther, host, ats, facia	nate number of nincludes any ocial security numbers, financare records and process, contil, hand, iris or records.	use or sha unique rec Electronic informatior umbers or icial accou d email add rol, use o etinal scar	bility) coverage any privious cords: cords: corecords: n or data the other gover unt number dresses. or share anns, DNA, or	at can be used nment identificas, personal ide	to unique ation num entification	ion* in e	y a person, yment card ers (PINs),	
	RE	CORDS (Complete Set Do you collect, store, or electronic form? If "Yes", provide the at Paper records: *Private or sensitive in including, but not limit information, drivers' usernames, passwords Do you collect, store fingerprints, voicepring characteristics that care	host, prapproximation ided to, so license is, healthout, host, ats, facia an be us	nate number of on includes any ocial security numbers, financare records and process, control, hand, iris or ried to uniquely	use or sha unique rec Electronic informatior umbers or icial accou d email add rol, use o etinal scar identify a p	bility) coverage any privious are are any privious are an	at can be used nment identificas, personal identificates, personal identificates, personal identificates, personal identificates, personal identificates, personal identificates, personal identificates and personal identificates and personal identificates and personal identificates are personal identificates and personal identificates are personal identificates and personal identificates are personal identificates are personal identificates and personal identificates are perso	to unique ation num entification formation gical, phy	ion* in e ly identifibers, pa n number or data	y a person, yment card ers (PINs), a, such as behavioral	☐ Yes ☐ No
	RE	CORDS (Complete Second Property Complete Secon	host, prapproximation ided to, so license is, healthout, host, facia an be us iewed you	nate number of on includes any ocial security numbers, financare records and process, control, hand, iris or ried to uniquely our policies relations.	use or sha unique rec Electronic informatior umbers or icial accoud d email add rol, use of etinal scar identify a p	bility) coverage any privious are are and any privious are any privious ar	at can be used nment identificate, personal i	to unique ation num entification formation ogical, phy	ion* in e ly identification bers, pa n number or data ysical or of such i	y a person, yment card ers (PINs), a, such as behavioral	
	RE	CORDS (Complete Set Do you collect, store, or electronic form? If "Yes", provide the at Paper records: *Private or sensitive in including, but not limit information, drivers' usernames, passwords Do you collect, store fingerprints, voicepring characteristics that cat If "Yes", have you rev	host, prapproximation ided to, so license is, healthout, host, facia an be us iewed you	nate number of on includes any ocial security numbers, financare records and process, control, hand, iris or ried to uniquely our policies relations.	use or sha unique rec Electronic informatior umbers or icial accoud d email add rol, use of etinal scar identify a p	bility) coverage any privious are are and any privious are any privious ar	at can be used nment identificate, personal i	to unique ation num entification formation ogical, phy	ion* in e ly identification bers, pa n number or data ysical or of such i	y a person, yment card ers (PINs), a, such as behavioral	
	RE	CORDS (Complete Section 2) Do you collect, store, or electronic form? If "Yes", provide the an electronic form? *Private or sensitive in including, but not limit information, drivers' usernames, passwords Do you collect, store fingerprints, voicepring characteristics that can lift "Yes", have you revor data with a qualifice	host, prapproximation approximation approxim	nate number of nincludes any ocial security numbers, financare records and process, control, hand, iris or red to uniquely our policies relancy and confirm	use or sha unique rec Electronic informatior umbers or icial accou d email add rol, use o etinal scar identify a l itting to the ned comp	bility) coverage any privious are are any	at can be used nment identificate, personal i	to unique ation num entification formation ogical, phy	ion* in e ly identification bers, pa n number or data ysical or of such i	y a person, yment card ers (PINs), a, such as behavioral	☐ Yes ☐ No
_	RE a.	Do you collect, store, or electronic form? If "Yes", provide the a Paper records: *Private or sensitive in including, but not limit information, drivers' usernames, passwords Do you collect, store fingerprints, voiceprin characteristics that calf "Yes", have you rev or data with a qualified laws?	host, prapproximation ided to, so license is, healthough, host, facia an be us iewed you ded attorned or handed.	nate number of nincludes any ocial security numbers, financare records and process, contil, hand, iris or red to uniquely our policies relancy and confirm	use or sha unique rec Electronic informatior umbers or icial accou d email add rol, use o etinal scar identify a l itting to the ned comp	bility) coverage any privious are are any	at can be used nment identificate, personal i	to unique ation num entification formation ogical, phy	ion* in e ly identification bers, pa n number or data ysical or of such i	y a person, yment card ers (PINs), a, such as behavioral	☐ Yes ☐ No
	b.	CORDS (Complete Section 2015) Do you collect, store, or electronic form? If "Yes", provide the an electronic form? *Private or sensitive in including, but not limit information, drivers' lusernames, passwords Do you collect, store fingerprints, voicepring characteristics that can lif "Yes", have you revor data with a qualified laws? Do you process, store	host, properties of the control of t	nate number of on includes any ocial security numbers, financare records and process, control, hand, iris or red to uniquely our policies related and confirm dle credit card to impliant?	use or sha unique rec Electronic informatior umbers or icial accou d email add rol, use of etinal scar identify a patting to the med comp	bility) coverage any privilence any privilence any privilence any privilence and a the other government number dresses. The share and the other government number dresses.	at can be used nment identificate, personal identificate, personal identificate, personal identificate, personal identificate, personal identification and other biologication and despilicable federage.	to unique ation num entification formation ogical, phy struction eral, state	ly identification bers, particular or data ysical or of such is a local a	y a person, yment card ers (PINs), a, such as behavioral nformation and foreign	 Yes □ No Yes □ No Yes □ No Yes □ No
4.	b.	Do you collect, store, or electronic form? If "Yes", provide the a Paper records: *Private or sensitive in including, but not limit information, drivers' usernames, passwords Do you collect, store fingerprints, voiceprincharacteristics that call "Yes", have you revor data with a qualified laws? Do you process, store If "Yes", are you PCI-	host, proposition of the design of the desig	nate number of on includes any ocial security numbers, financare records and process, control, hand, iris or red to uniquely our policies related to uniquely our pol	use or sha unique rec Electronic informatior umbers or icial accou d email add rol, use of etinal scar identify a patting to the med comp	bility) coverage any privilence any privilence any privilence any privilence and a the other government number dresses. The share and the other government number dresses.	at can be used nment identificate, personal identificate, personal identificate, personal identificate, personal identificate, personal identification and other biologication and despilicable federage.	to unique ation num entification formation ogical, phy struction eral, state	ly identification bers, particular or data ysical or of such is a local a	y a person, yment card ers (PINs), a, such as behavioral nformation and foreign	 Yes □ No Yes □ No Yes □ No Yes □ No

CBO-NBA (11.2021) Page **1** of **7**

	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.						
		If "Yes", when was it impleme	nted?				
		If "No", do you outsource your billings to a third-party billing company?					
	f.	Do you use credentialed staff to perform billing procedures?					
		If Yes", how many credentiale	d staff members do you employ for this purpose? _				
	g.	Do you bill all services under t	ne 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?					
	h.	Is your practice using a currer	nt edition of the CPT manual?		☐ Yes ☐ No		
	i.	Is software used to ensure bil	ling compliance?		☐ Yes ☐ No		
		If "Yes", when was the softwa	re installed?				
	j.		is responsible for billing compliance? Please include v often such person performs billing compliance revi				
6.	IT [DEPARTMENT (Complete Sec	ction 6 only if e-MD (Cyber Liability) coverage is	desired.)			
	Thi: use	s section must be completed b d in this section only, "you" ref	the individual within the Applicant's organization weers only to such individual.	ho is responsible for network	security. As		
	a.	Within the Applicant's organiz	ation, who is responsible for network security?				
		Name:					
		Title:					
		Phone: Email address:					
		IT Security Designation(s):					
	b. The Applicant's network security is: ☐ Outsourced; provide the name of your network security provider:						
			☐ Managed internally/in-house				
	C.	named in question b. above?	urity is outsourced, are you the main contact for the	e network security provider	☐ Yes ☐ No		
			email address for the main contact:				
	d.	How many IT personnel are o	•				
	е.		ity 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.							
Prir	Print/Type Name:						
Sig	Signature:						
7.			Complete Section 7 only if e-MD (Cyber Liability)	•			
			is section is "No", please provide additional details in				
	a.	• •	alert employees that the message originated from o	outside the organization?	☐ Yes ☐ No		
	b.	If "Yes", complete the following	potentially malicious attachments and links?		☐ Yes ☐ No		
		(1) Select your email security					
		•	me of your email security provider:				
		(2) Do you have the capabilit	y to automatically detonate and evaluate attachment to delivery to the end-user?	s in a sandbox to determine	☐ Yes ☐ No		

CBO-NBA (11.2021) Page **2** of **7**

	c.	Have you implemented any of the following to protect against phishing messages? (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			
		<u>NAL COMMENTS</u> (Use this space to explain any "No" answers in the above section and/or to list other rele s you are utilizing that are not listed here.)	vant II security			
mea	Surce	s you are unitering that are not hated here.)				
8.	INT	ERNAL SECURITY CONTROLS (Complete Section 8 only if e-MD (Cyber Liability) coverage is desired.)				
	If th	e 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?	☐ Yes ☐ No			
		If "Yes", provide the name of the cloud provider:				
		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.				
	C.	Do you use MFA to secure all cloud provider services that you utilize (e.g. Amazon Web Services (AWS),				
	<u> </u>	Microsoft Azure, Google Cloud)?	☐ Yes ☐ No			
	d.	Do you encrypt all sensitive and confidential information stored on your organization's systems and networks?	☐ Yes ☐ No			
		If "No", are the following compensating controls in place:	☐ Yes ☐ No			
		(1) Segregation of servers that store sensitive and confidential information?(2) Access control with role-based assignments?	☐ Yes ☐ No			
	e.	Do you allow remote access to your network?	☐ Yes ☐ No			
	•	If "Yes", do you use MFA to secure all remote access to your network, including any remote desktop protocol				
		(RDP) connections?	☐ Yes ☐ No			
		If MFA is used, complete the following:				
		(1) Select your MFA provider: Choose an item.				
		If "Other", provide the name of your MFA provider:				
		(2) Select your MFA type: Choose an item.				
		If "Other", describe your MFA type:				
		(3) Does your MFA configuration ensure that the compromise of a single device will only compromise a				
	_	single authenticator?	Yes No			
	f.	Do you use a next-generation antivirus (NGAV) product to protect all endpoints across your enterprise? If "Yes", complete the following:	☐ Yes ☐ No			
		·				
		(1) Select your NGAV provider: Choose an item.				
		If "Other", provide the name of your NGAV provider:				
		(2) Do you enforce application whitelisting/blacklisting?	☐ Yes ☐ No			
		(3) Is an endpoint detection and response (EDR) tool deployed on 100% of endpoints?	☐ Yes ☐ No			
		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.				
		(4) Can users access the network with their own device ("Bring Your Own Device")?	☐ Yes ☐ No			
		If "Yes", is EDR required to be installed on these devices?	☐ Yes ☐ No			

CBO-NBA (11.2021) Page **3** of **7**

g.	Do you use an EDR tool that includes centralized monitoring and logging of all endpoint activity across your	
	enterprise?	☐ Yes ☐ No
	If "Yes", complete the following:	
	(1) Select your EDR provider: Choose an item.	
	If "Other", provide the name of your EDR provider:	
	(2) Do you enforce application whitelisting/blacklisting?	☐ Yes ☐ No
	(3) Is EDR deployed on 100% of endpoints?	☐ Yes ☐ No
	If "No", please use the Additional Comments section to outline which assets do not have EDR , and whether any mitigating safeguards are in place for such assets.	
	(4) Can users access the network with their own device ("Bring Your Own Device")?	☐ Yes ☐ No
	If "Yes", is EDR required to be installed on these devices?	☐ Yes ☐ No
h.	Do you use MFA to protect all local and remote access to privileged user accounts?	☐ Yes ☐ No
	If "Yes", select your MFA type: Choose an item.	
	If "Other", describe your MFA type:	
i.	Do you manage privileged accounts using privileged account management software (PAM) (e.g., CyberArk, BeyondTrust, etc.)?	☐ Yes ☐ No
	If "Yes", complete the following:	
	(1) Provide the name of your software provider:	
	(2) Is access protected by MFA?	☐ Yes ☐ No
j.	Do you actively monitor all administrator access for unusual behavior patterns?	☐ Yes ☐ No
	If "Yes", provide the name of your monitoring tool:	
k.	Do you roll out a hardened baseline configuration across servers, laptops, desktops and managed mobile	
	devices?	☐ Yes ☐ No
I.	Do you record and track all software and hardware assets deployed across your organization?	∐ Yes ∐ No
	If "Yes", provide the name of the tool used for this purpose (if any):	
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	
0.	Do you have any end of life or end of support software?	☐ Yes ☐ No
	If "Yes", is it segregated from the rest of your network?	☐ Yes ☐ No
p.	Do you use a protective DNS service (PDNS) (e.g. ZScaler, Quad9, OpenDNS or the public sector PDNS)	
ρ.	to block access to known malicious websites?	☐ Yes ☐ No
	If "Yes", provide the name of your DNS provider:	
q.	Do you use endpoint application isolation and containment technology on all endpoints?	☐ Yes ☐ No
	If "Yes", select your provider: Choose an item.	
	If "Other", provide the name of your provider:	
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 <u>Environment Recommendations by Microsoft?</u>	Yes No
t.	Do you utilize a Security Information and Event Management system (SIEM)?	☐ Yes ☐ No
u.	Do you utilize a Security Operations Center (SOC)?	☐ Yes ☐ No
	If "Yes", complete the following:	
	(1) Is your SOC monitored 24 hours a day, 7 days a week?	☐ Yes ☐ No
	(2) Your SOC is: ☐ Outsourced; provide the name of your provider: ☐ Managed internally/in-house	
V.	Do you use a vulnerability management tool?	☐ Yes ☐ No
	If "Yes", complete the following:	
	(1) Select your provider: Choose an item.	
	If "Other", provide the name of your provider:	
	(2) What is your patching cadence?	
	☐ 1-3 days ☐ 4-7 days ☐ 8-30 days ☐ 1 month or longer	

CBO-NBA (11.2021) Page **4** of **7**

		NAL COMMENTS (Use this space to explain any "No" answers in the above section and/or to list other re s you are utilizing that are not listed here.)	levant IT security
9.	RΔ	CKUP AND RECOVERY POLICIES (Complete Section 9 only if e-MD (Cyber Liability) coverage is desired	1)
0.		e answer to the question in this section is "No", please provide additional details in the "Additional Comments".	•
		you use a data backup solution?	☐ Yes ☐ No
	lf "۱	'es":	
	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	
		NAL COMMENTS (Use this space to explain any "No" answers in the above section and/or to list other relevant	
II SE	curi	ty measures you are utilizing that are not listed here.)	
10.	рш	SUINC CONTROLS (Complete Section 10 only if a MD (Cyber Lightlity) coverage is decired.)	
10.	а.	SHING CONTROLS (Complete Section 10 only if e-MD (Cyber Liability) coverage is desired.) Do any of the following employees at your company complete social engineering training:	
	a.	(1) Employees with financial or accounting responsibilities?	□ Vaa □ Na
		(2) Employees <u>without</u> 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	☐ Yes ☐ No
		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 before the change request was received?	☐ Yes ☐ No

CBO-NBA (11.2021) Page **5** of **7**

11.	RE	GUL	ATORY LOSS HISTORY (Co	mplete Section 11 only if	MEDEFENSE Plus (Regulatory) coverage is de	esired.)
	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.		er internal inquiry, have you, urance, any consultant, or any		ff, any other person or entity proposed for this you perform billing services:	
		(1)	Had to refund amounts to go years?	overnment (public) and/or o	commercial (private) payers within the past three	☐ Yes ☐ No
			If "Yes", provide estimated a	mounts:		☐ Tes ☐ NO
			Current Year (Fiscal):	Public: \$	_ Private: \$	
			Last Year (Fiscal):	Public: \$	_ Private: \$	
			Two Years Ago (Fiscal): Pub	olic: \$	Private: \$	
					of improper billing or voluntary self-disclosure?	☐ Yes ☐ No
		(2)	Been placed on prepayme commercial payer?	nt review by any local, s	state or federal government agency or by any	☐ Yes ☐ No
		(3)		Medicaid billing practices,	ate or federal government agency or commercial utilization of Medicare/Medicaid services or the eof?	☐ Yes ☐ No
		(4)	Been sued or deselected by	a commercial payer?		☐ Yes ☐ No
		(5)	Been reviewed, investigated	or sanctioned by a state m	nedical licensing board?	☐ Yes ☐ No
		(6)	Been investigated for HIPAA	λ, EMTALA or Stark/anti-kic	ckback violations?	☐ Yes ☐ No
	b.				or this insurance have knowledge of any facts,	
			umstances, situations, event estigation or demand for restit		result in a medical regulatory action, regulatory	☐ Yes ☐ No
12.	CY	BER	PRIVACY LOSS HISTORY (Complete Section 12 only	y if e-MD (Cyber Liability) coverage is desired.)	
			swer to any question in 12.a n or incident.	. through 12.c. below is "Y	es", please complete a Claim Supplemental Form	າ for each claim,
	a.	In th	ne past 3 years, has the Appli	cant or any other person or	r organization proposed for this insurance:	
		(1)	injury, breach of private info	rmation, network security, mputer virus infections, the	a subject in litigation involving matters of privacy defamation, content infringement, identity theft, eft of information, damage to third party networks etwork?	☐ Yes ☐ No
		(2)	Been the subject of any goviolation of privacy law or reg	vernment action, investigat gulation?	tion or other proceedings regarding any alleged	☐ Yes ☐ No
		(3)	Notified customers, clients o	r any third party of any sec	urity breach or privacy breach?	☐ Yes ☐ No
		(4)	Received any cyber extortion	n demand or threat?		☐ Yes ☐ No
		(5)	Sustained any unscheduled	network outage or interrupt	tion for any reason?	☐ Yes ☐ No
		(6)	Sustained any property dama	age or business interruption	n losses as a result of a cyber-attack?	☐ Yes ☐ No
		(7)	Sustained any losses due to	wire transfer fraud, telecon	mmunications fraud or phishing fraud?	☐ Yes ☐ No
	b.	brea			this insurance have knowledge of any security allegations of breach of privacy that may give rise	☐ Yes ☐ No
	C.		ne past 3 years, has any serv tained an unscheduled netwo		o the Applicant's network or computer system(s) sting longer than 4 hours?	☐ Yes ☐ No
		If "Y	es", did the Applicant experie	ence an interruption in busir	ness as a result of such outage or interruption?	☐ Yes ☐ No
NOT	ICE	TO A	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.						
CON	IPA	NY C	OR OTHER PERSON FILES	AN APPLICATION FOR	DWINGLY AND WITH INTENT TO DEFRAUD AI INSURANCE CONTAINING ANY FALSE INFO N CONCERNING ANY FACT MATERIAL THERE	ORMATION, OR

CBO-NBA (11.2021) Page **6** of **7**

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

CBO-NBA (11.2021) Page **7** of **7**

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.



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

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.

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™

