Tulare Local Healthcare District dba Tulare Regional Medical Center

Agenda Item

Board Meeting Date:

October 3, 2018

Title to Appear on Agenda:

Request Approval for Cyber Insurance Coverage Policy

Brief Description:

The Interim Management Services Agreement between Adventist Health and Tulare Local Healthcare District requires the District to obtain several types of Insurance coverage, including Privacy (Cyber Risk) Liability coverage.

Background and Details:

The Districts' Insurance Brokers, Marsh and McLennan, have "shopped" for this coverage, and are recommending NAS/Underwriting at Lloyd's.

Coverage limits will be $3M, and Dependent System Failure Limits can be increased from $1M to $3M for an additional 15% of premium. The District's I/T Consulting firm recommends that this incremental coverage be purchased.

Exhibits:

A copy of the Marsh McLennan proposal is included as an Exhibit.

Recommended Action:

That the District authorize purchase of the Cyber insurance as outlined (Premium of $22,047), including an additional $3,307.05 for the increase in the Dependent System Failure Limits coverage from $1M to $3M.

MARSH & McLENNAN AGENCY

TULARE LOCAL HEALTH CARE DISTRICT DBA: TULARE REGIONAL MEDICAL CENTER

PROPOSAL FOR INSURANCE SERVICES

CYBER LIABILITY / DATA BREACH RESPONSE COVERAGE

EFFECTIVE: TBD

CONTENTS

INTRODUCTION:

SPECIFICATIONS:

ADDENDUM:

DIRECTORY

PRINCIPAL:	**Bill Buchanan** (858) 587-7567 bill.buchanan@MarshMMA.com
CLIENT EXECUTIVE:	**Jim Gonzales** (858) 550-1147 jim.gonzales@MarshMMA.com
CLIENT MANAGER:	**Drisana Wallace** (858) 750-4520 drisana.wallace@MarshMMA.com
DIRECTOR OF RISK & LOSS ADVISORS:	**Jeff Hulson** (858) 550-4987 jeff.hulson@MarshMMA.com
WORKERS' COMPENSATION SPECIALIST:	**Carrie Stern** (858) 875-3076 carrie.stern@MarshMMA.com
EMPLOYEE BENEFITS:	**Steve Finden** (858) 587-7405 steve.finden@MarshMMA.com
PENSION & RETIREMENT SERVICES:	**Bill Peartree** (858) 550-4978 bill.peartree@MarshMMA.com
CONTROLLER:	**Dane Bustrum** (858) 587-7493 dane.bustrum@MarshMMA.com
HEADQUARTERS:	**San Diego Office** P.O. Box 85638 San Diego, CA 92186-5638 9171 Towne Centre Dr., Ste. 500 San Diego, CA 92122 Phone: (858) 457-3414 / (800) 321-4696 Fax: (858) 452-7530 www.MarshMMA.com

MARKETING SUMMARY

INSURANCE COMPANY	RESULTS	ADDITIONAL COMMENTS
NAS (Lloyds)	Quoted	Premium: $22,047 Limit: $3,000,000 Retention: $25,000

***PREMIUM INCLUDES TAXES/FEES**

NAMED INSURED

- Tulare Local Health Care District DBA: Tulare Regional Medical Center

MAILING ADDRESS

869 N. Cherry St.
Tulare, CA 93274

This is our understanding of your entire list of named insureds. This list may or may not appear on every policy. Each policy should be reviewed to confirm the appropriate list of named insureds.

CYBER LIABILITY / DATA BREACH RESPONSE COVERAGE

Carrier Name: NAS/ Underwriters at Lloyd's (Non-Admitted)

A.M. Best Rating: A, XV

POLICY NUMBER

TBD

POLICY PERIOD

TBD

POLICY FORM

- Claims Made: All claims must be reported as soon as practicable. Circumstances that may lead to a claim may be reported under this policy period. Subsequent claim will be deemed to have been made during policy period.
- $1,000,000 Defense Costs Outside the limit
- Retroactive Date: None. Unknown Prior Acts Covered.

LIMITS OF INSURANCE

Policy Aggregate Liability Limit	$3,000,000 Aggregate
Additional Defense Costs Limit (only for Insuring agreements I- IV)	$1,000,000
Third Party Liability Insuring Agreements	
Multimedia Liability	$3,000,000 Each Claim/ Aggregate
Security and Privacy Liability	$3,000,000 Each Claim/ Aggregate
Privacy Regulatory Defense and Penalties	$3,000,000 Each Claim/ Aggregate
PCI DSS Liability	$3,000,000 Each Claim/ Aggregate
TCPA Defense	$50,000 Each Claim/ Aggregate

First Party Insuring Agreements	
Breach Event Costs	$3,000,000 Each Claim/ Aggregate
Post Remediation Costs	$25,000 Each Claim/ Aggregate
BrandGuard	$3,000,000 Each Claim/ Aggregate
System Failure	$3,000,000 Each Claim/ Aggregate
Dependent System Failure	$1,000,000 Each Claim/ Aggregate
Cyber Extortion	$3,000,000 Each Claim/ Aggregate
Cyber Crime	$1,000,000 Each Claim/ Aggregate
Reward Expense	$50,000 Each Claim/ Aggregate
Court Attendance Costs	$25,000 Each Claim/ Aggregate

CYBER LIABILITY / DATA BREACH RESPONSE COVERAGE (CONTINUED)

RETENTIONS

Retention (applies to all coverage parts but those below)	$25,000
BrandGuard Waiting Period/ Period of Indemnity	Waiting Period: 2 Weeks Period of Indemnity: 6 Months
System Failure- Non-physical Business Interruption Waiting Period/ Period of Indemnity	Waiting Period: 8 Hours Period of Restoration: 6 Months
Dependent System Failure- Non-physical Business Interruption Waiting Period/ Period of Indemnity	Waiting Period: 12 Hours Period of Restoration: 4 Months

SURPLUS LINES NOTIFICATION

This policy is quoted with a non-admitted insurance carrier. The insurer is not admitted or licensed by your Home State. As such, insureds under this policy are not protected by any state guaranty fund in the event of the insurer becomes insolvent. Surplus Lines taxes and fees may apply and are subject to change based upon respective Home State NRRA regulatory updates.

CLAIMS MADE NOTIFICATION

Claims under this policy must be submitted by you to the Insurer during the policy period, or within a specific number of days as stated in the policy, after the expiration of the policy, for coverage to apply.

CONTINGENCIES

Signed/dated D-1 within 7 days of binding

Completed VMW (if full limits for DSF is desired for 15% A/P)- Due PRIOR TO BINDING

CYBER LIABILITY / DATA BREACH RESPONSE COVERAGE (CONTINUED)

GLOSSARY OF KEY COVERAGE TERMS

Multimedia Liability- intends to provide party coverage for:

- ✓ **Multimedia Wrongful Act** defined as the following as the direct result of dissemination of media material by an insured:
  - o any form of defamation or other tort related to the disparagement or harm to the reputation or character of any person or organization, including libel, slander, product disparagement or trade libel, and infliction of emotional distress, mental anguish, outrage or outrageous conduct, if directly resulting from any of the foregoing;
  - o invasion, infringement or interference with an individual's right of privacy or publicity, including the torts of false light, intrusion upon seclusion, commercial misappropriation of name, person, or likeness, and public disclosure of private facts;
  - o plagiarism, piracy or misappropriation of ideas under an implied contract;
  - o infringement of copyright, trademark, trade name, trade dress, title, slogan, service mark or service name;
  - o domain name infringement or improper deep-linking or framing;
  - o negligence in media material, including a claim alleging harm to any person or entity that acted or failed to act in reliance upon such media material; 7) false arrest, detention or imprisonment; 8) trespass, wrongful entry or eviction, eavesdropping, or other invasion of the right of private occupancy;
  - o unfair competition, but only when arising out of a peril described in 1. through 8. above.

Security and Privacy Liability- intends to provide coverage for: the following whether actual or alleged, but only if committed by an insured:

- ✓ The failure to prevent or hinder a security breach, which in turn results in:
  - o The alteration, copying, corruption, destruction, deletion, or damage to data stored on an insured computer system;
  - o Theft, loss or unauthorized disclosure of electronic or non-electronic private information that is in your care, custody or control;
  - o Theft, loss or unauthorized disclosure of electronic or non-electronic private information that is in the care, custody or control of a BPO service provider or outsourced IT service provider that is holding, processing or transferring such private information on your behalf; provided there is an existing written contract with such BPO service provider or outsourced IT provider
  - o Unauthorized access to, or unauthorized use of, a computer system other than an insured computer system;
  - o The inability of an authorized third party to gain access to your services;
- ✓ The failure to timely disclose a security breach or privacy breach affecting private information;
- ✓ The failure to dispose of private information within the required period, in violation of privacy regulations;
- ✓ The failure to prevent the transmission of malicious code or computer virus from an insured computer system to the computer system of a third party;
- ✓ A privacy breach;
- ✓ The failure to prevent a privacy breach;

- ✓ The failure to prevent or hinder participation by an insured computer system in a denial of service attack directed against the internet site or computer system of a third party;
- ✓ The failure to prevent the theft or loss of personally identifiable information of employees; or
- ✓ Infliction of emotional distress or mental anguish, but only if directly resulting from a peril described in paragraphs 1. through 8. above.
- ✓ **Security breach** means any of the following, whether a specifically targeted attack or a generally distributed attack:
  - a hacking attack;
  - the physical theft or loss of an unsecured data storage device containing private information; or the theft or loss of an unsecured mobile or handheld device containing private information, including any smartphone, tablet, and laptop owned by you and operated by an insured, or owned and operated by an employee or executive who has agreed in writing to your corporate mobile device acceptable use and security policy (also known as a "Bring Your Own Device" policy) first of
- ✓ **Privacy Breach**- defined as:
  - The unauthorized collection, disclosure, use, access, destruction or modification of private information;
  - The inability to access, or failure to provide, private information;
  - The theft or loss of private information, including the theft or loss of private information stored on an unsecured data storage device or mobile or handheld device, including any smartphone, tablet, and laptop which is owned by you and operated by an Insured, or owned and operated by an employee or executive – who has a BYOD policy.
  - The surrender of private information in a phishing attack;
  - Failure to implement, maintain, or comply with privacy policies and procedures stating your obligations relating to private information, including but not limited to your privacy policy;
  - Failure to develop or administer an identity theft prevention program;
  - Failure to implement specific security practices with respect to private information required by any statute, rule, regulation, or other law;
  - An infringement or violation of any rights to privacy;
  - Breach of a person's right of publicity, false light, or intrusion upon a person's seclusion;
  - Failure to comply with privacy regulations pertaining to an Insured's responsibilities with respect to private information, but only with respect to an act listed in paragraphs 1 through 8 above; or
  - Failure to comply with privacy regulations prohibiting unfair or deceptive trade practices or consumer fraud pertaining to an Insured's responsibilities with respect to private information, but only with respect to an act listed in paragraphs 1 through 8 above.

Privacy Regulatory Defense and Penalties- intends to provide coverage for:

- ✓ Regulatory compensatory award or fines and penalties as the result of a privacy regulatory proceeding

PCI DSS Liability- intends to provide coverage for the following as the result of a PCI Demand:

- ✓ PCI DSS fines and assets and related defense costs
- ✓ PCI Demand defined As:

TCPA Defense- intends to provide coverage for:

- ✓ Defense costs only for a TCPA Claim; which is defined as:
  - A written demand made against an Insured for money or non-monetary relief alleging a TCPA violation;
  - The service of a civil lawsuit or the institution of arbitration or other alternative dispute resolution proceedings against an Insured alleging a TCPA violation and seeking money, a temporary restraining order, or a preliminary or permanent injunction; or
  - A written request received by an Insured to toll or waive a statute of limitations relating to a potential TCPA claim against an Insured.

Breach Events Costs- intends to provide coverage for the following g the result of an adverse media report (report/communication of a potential security and privacy breach), security breach or privacy breach

- ✓ **Privacy breach Costs**
  - Initial breach consultation costs;
  - Reasonable and necessary public relations expenses
  - Reasonable and necessary legal fees that you incur on your own behalf or on behalf of a party for whom you are vicariously liable to:
    - Determine the scope, cause, and extent of an actual or suspected privacy breach or security breach;
    - Determine the applicability of, and your obligations to comply with, privacy regulations due to an actual or suspected privacy breach; and
    - Draft a notification letter to be sent to parties affected by a privacy breach.
  - Reasonable and necessary fees and costs that you incur on your own behalf, or on behalf of a party for whom you are vicariously liable, to retain a qualified IT forensics firm or computer security expert to investigate and identify the source and scope of a security breach or privacy breach; and
  - Overtime salaries of non-exempt employees assigned to handle inquiries from parties affected by a privacy breach.
- ✓ **Notification Expense:**
- ✓ **Breach support and credit monitoring** (with approval):
  - reasonable and necessary expenses you incur on your own behalf, or on behalf of a party for whom you are vicariously liable, to provide support activity to parties affected by a privacy breach. Breach support and credit monitoring expenses includes the cost to set up a call center and to provide a maximum of twenty-four (24) months of credit monitoring services, identity theft assistance services, or credit or identity repair and restoration services

Post Breach Remediation Costs- intends to provide coverage for costs to:

- ✓ Help mitigate the potential of future security breach or privacy breach, including, but not limited to security risk assets, development an information security doc set, employee training etc.

BrandGuard- intends to provide coverage for:

- ✓ Provable and ascertainable brand loss sustained during the period of indemnity as a direct result of an adverse media report or notification as the result of a security breach or privacy breach

System Failure- intends to provide coverage for:

- ✓ **Data recovery**- which extends coverage to digital asset loss and special expenses as the result of damage, alteration, corruption, distortion, theft, misuse or destruction of digital assets are the result of a system failure
  - o **Digital Asset Loss** defined as: reasonable and necessary expenses and costs you incur to replace, recreate or restore digital assets to the same state and with the same contents immediately before the digital assets were damaged, destroyed, altered, misused, or stolen, including expenses for materials and machine time. Also includes amounts representing employee work time to replace, recreate or restore digital assets, which will be determined on a predefined billable hour or per-hour basis as based upon your schedule of employee billable hours
- ✓ **System failure** defined as:
  - o an unplanned outage, interruption, failure, suspension, or degradation of service of an insured computer system, including, but not limited to, any such outage, interruption, failure, suspension, or degradation of service caused directly by a hacking attack.
- ✓ **Non-physical business interruption**- extends coverage for income loss, interruption expenses and special expenses incurred during the period of restoration because of a system failure

Dependent System Failure- intends to extend system failure coverage for the following:

- ✓ an unplanned outage, interruption, failure, suspension, or degradation of service of a service provider computer system

Cyber Extortion- intends to provide coverage for the following a result of a cyber extortion threat

- ✓ **Cyber extortion expenses-** includes the costs to retain or hire third party specializing in IT security to determine the validity and severity of the threat
- ✓ **Cyber extortion monies**- includes bitcoin or digital currency
- ✓ **Cyber Extortion Threat** Classified as a credible threat (or series of such) to:
  - o steal, alter, release, reveal, divulge, disseminate, destroy, publicly disclose, or misuse private information taken from an Insured through unauthorized access to, or unauthorized use of, an insured computer system;
  - o infect an insured computer system with malicious code or ransomware;
  - o corrupt, damage or destroy an insured computer system;
  - o restrict or hinder access to an insured computer system, including the threat of a denial of service attack;
  - o perpetrate or carry out a phishing attack;
  - o steal, alter, release, reveal, divulge, disseminate, destroy, publicly disclose, or misuse your confidential or proprietary information, or the personally identifiable information of an insured;
  - o or damage your reputation or your brand by posting false or misleading comments about you or your organization on social media websites or platform

Cyber Crime- intends to provide coverage for:

- ✓ **Financial Fraud-** intended to provide coverage for the following:
  - o an intentional, unauthorized and fraudulent written, electronic or telephonic instruction transmitted to a financial institution, directing such institution to debit your account and to debit, transfer, pay or deliver money or securities from your account, which instruction

purports to have been transmitted by you, an executive, or an employee, but was in fact fraudulently transmitted by a third party without your knowledge or consent; or
  - the theft of money or securities from your account or your corporate credit cards as a result of a hacking attack.
- ✓ **Telecommunications Fraud** Provide coverage for the charges you incur for unauthorized calls resulting from:
  - the intentional, unauthorized and fraudulent gaining of access to outgoing telephone service through infiltration and manipulation of an insured telecommunications system.
- ✓ **Phishing Attack -** intended to provide coverage for the following via the the use by a third party of fraudulent telephone calls, emails, texts, instant messages or other electronic communications or malicious websites to impersonate you, your brand, or your products or services to solicit private information:
  - direct financial loss you sustain due to a phishing attack that fraudulently induces an executive or employee to transfer, pay or deliver money, securities, or other property to an unintended third party;
  - expenses you incur with approval to create and issue a specific press release or to establish a specific website to advise your customers and prospective customers of a phishing attack; and
  - the cost of reimbursing your existing customers or clients for their direct financial losses resulting from a phishing attack, provided such reimbursement is made by you with approval

Reward Expenses- intends to provide coverage for:

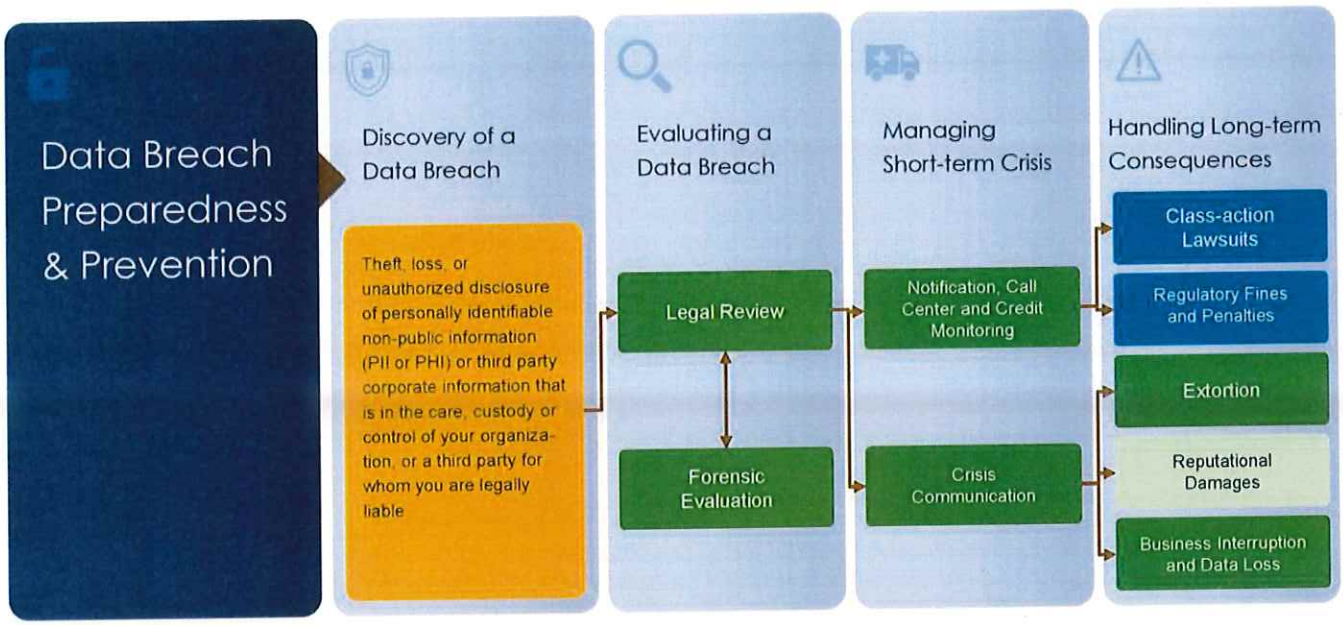
- ✓ rreasonable amount that you pay with approval to an informant for information not otherwise available which leads to the arrest and conviction of any person who commits an illegal act that causes a first party insured event.
- ✓

Court Attendance- intends to provide coverage for:

- ✓ Court attendance costs; $500 per date;

The descriptions above are general descriptions to assist you in better understanding this coverage. Please review the actual policy forms for the specific details. As with any policy, these key terms are subject to exclusions, definitions and other provisions that can limit how the coverage is to be applied.

CYBER LIABILITY / DATA BREACH RESPONSE COVERAGE (CONTINUED)



DESCRIPTION OF NAS BREACH RESPONSE SERVICES

NAS Insurance Cyber Liability Solutions go beyond the breach to provide complete risk management, breach response and reputation recovery. Their NetGuard Plus cyber liability insurance provides comprehensive first- and third-party coverages for a broad range of network security and privacy risks. Brand Guard coverage provides the resources you need to swiftly recover and restore your business to profitability.

NAS simplifies cyber breach response with one-call claims services. They have a nationwide network of legal, IT, Crisis Management and customer notification service providers are coordinated by a dedicated Cyber Breach Coach to provide a custom-tailored response to your specific and local needs. There is no one-size-fits-all approach when it comes to your business. Coverage provided includes access to:

- Forensic experts
  Legal services
  Notification services
  Public relations and crisis management
  Call center services
  Credit / Identity monitoring

  Beyond that you will receive access to an online portal which provides online compliance manuals, training programs, step-by-step procedures to reduce risk and action to take when a breach occurs.

CYBER LIABILITY / DATA BREACH RESPONSE COVERAGE (CONTINUED)

EXCLUSIONS/ENDORSEMENTS

- Per Policy Form; Including But Not Limited To:
  - Unlawful collection, acquisition or retention of personally identifiable information
  - Antitrust, Unfair Competition
  - Prior acts – None. Unknown Prior Acts Covered
  - Intentional Dishonest / Fraudulent / Criminal / Malicious Acts – final adjudication wording
  - Patent, trade secrets, software code copyright

Added Enhancements:

- $250K Bodily Injury Sublimit
- RT Amendatory:
  - Amends definition of application, to only limited what was submitted for this policy
  - Amends definition of executive to ONLY include: CEO, CFO, COO, CTO, CIO, CPO, GC or other in-house lawyer and risk manager (or those in functionality equivalent roles)
  - Amends Definition of Outsourced It to no longer exclude payment processor or security software provider
  - Amends definition of Privacy breach to remove the criteria for the stored data to be on an "unsecured" device
  - Amends Definition of Privacy regulation definition to also apply to the "collection" of private information
  - Amends Definition of Security and privacy Wrongful Act to move the careveback that: that the theft, loss or unauthorized disclosure occurs while your written contract with such BPO service provider or outsourced IT service provider is still in effect;
  - Amends definition of Security breach to remove the requirement for the storage device containing private information to be "unsecured"
  - Amend the Prior Notice Exclusion; to read " earlier of the effective date" of this policy; in lieu of or "prior to " the effective date of a policy issued
  - Amend Breach of Contract Exclusion to remove "promise" from the carevbacks
  - Amend the Securities Exclusion to only exclude:
    - Violation of any rules or regulations promulgated under securities laws concerning the security, access, and use of private information; or
    - Failure to safeguard private information obtained by an insured in the course of a securities transaction.
  - Amend the TCPA, Can-Spam Exclusion, etc. exclusion to provide a carevback for the following under insuring agreement II :
    - alleging violation by an Insured of the CAN-SPAM Act, as amended, or any regulation promulgated thereunder, or any similar federal, state, local or foreign

law, but only if such violation is unintentional and a consequence of a hacking attack
- Amends the ERP election window from 30 days to 60 days post
- Amend Notice Provision window to after an executive(note the definition of executive as amended above) first becomes aware of the claim and/or the first party event giving rise to the claim
- Amend other insurance clause, for this policy to sit primary
- Only cancellable for non-payment
- Removes the written requirement by the insured for creation or acquisition of a subsidiary
- Removes the written requirement by the insured to notify in the event of a sold subsidiary
- Amends coverage in the event of a takeover and change of control with ERP window to a 60 day election window
- Amends the Warranty by the Named insured to read:
  - In the event the application, or any supplemental materials submitted to the Underwriters therewith, contains any misrepresentation or omission made with the intent to deceive, or which materially affects either the acceptance of the risk or hazard assumed by the Underwriters under this Policy, this Policy will be null and void *ab initio* as to any Insured who knew the facts misrepresented or the omission, whether or not such person knew of the application or this Policy. The knowledge of an Insured will not be imputed to any other Insured.

CONDITIONS

- All claims must be reported as soon as practicable, but no later than 60 days post expiration upon: any insured's notice
- Defense costs incurred before notice of a claim to insurer, without the insurer's written approval or by unapproved counsel may not be paid.
- Email notices to: claims@nasinsurance.com

Mail a copy to: Marsh & McLennan Insurance Agency LLC
ATTN: Claims Department
9171 Towne Centre Dr., Ste. 500
San Diego, CA 92122

COMPENSATION DISCLOSURE

Marsh & McLennan Agency LLC ("MMA") prides itself on being an industry leader in the area of transparency and compensation disclosure. We believe you should understand how we are paid for the services we are providing to you. We are committed to compensation transparency and to disclosing to you information that will assist you in evaluating potential conflicts of interest.

As a professional insurance producer, MMA and its subsidiaries facilitate the placement of insurance coverage on behalf of our clients. As an independent insurance agent, MMA may have authority to obligate an insurance company on behalf of our clients and as a result, we may be required to act within the scope of the authority granted to us under our contract with the insurer. In accordance with industry custom, we are compensated either through commissions that are calculated as a percentage of the insurance premiums charged by insurers, or fees agreed to with our clients.

MMA receives compensation through one or a combination of the following methods:

Retail Commissions – A retail commission is paid to MMA by the insurer (or wholesale broker) as a percentage of the premium charged to the insured for the policy. The amount of commission may vary depending on several factors, including the type of insurance product sold and the insurer selected by the client.

Client Fees – Some clients may negotiate a fee for MMA's services in lieu of, or in addition to, retail commissions paid by insurance companies. Fee agreements are in writing, typically pursuant to a Client Service Agreement, which sets forth the services to be provided by MMA, the compensation to be paid to MMA, and the terms of MMA's engagement. The fee may be collected in whole, or in part, through the crediting of retail commissions collected by MMA for the client's placements.

Contingent Commissions – Many insurers agree to pay contingent commissions to insurance producers who meet set goals for all or some of the policies the insurance producers place with the insurer during the current year. The set goals may include volume, profitability, retention and/or growth thresholds. Because the amount of contingent commission earned may vary depending on factors relating to an entire book of business over the course of a year, the amount of contingent commission attributable to any given policy typically will not be known at the time of placement.

Supplemental Commissions – Certain insurers and wholesalers agree to pay supplemental commissions, which are based on an insurance producer's performance during the prior year. Supplemental commissions are paid as a percentage of premium that is set at the beginning of the calendar year. This percentage remains fixed for all eligible policies written by the insurer during the ensuing year. Unlike contingent commissions, the amount of supplemental commission is known at the time of insurance placement. Like contingent commissions, they may be based on volume, profitability, retention and/or growth.

Wholesale Broking Commissions – Sometimes MMA acts as a wholesale insurance broker. In these placements, MMA is engaged by a retail agent that has the direct relationship with the insured. As the wholesaler, MMA may have specialized expertise, access to surplus lines markets, or access to specialized insurance facilities that the retail agent does not have. In these transactions, the insurer typically pays a commission that is divided between the retail and wholesale broker pursuant to arrangements made between them.

Other Compensation – From time to time, MMA may be compensated by insurers for providing administrative services to clients on behalf of those insurers. Such amounts are typically calculated as a percentage of premium or are based on the number of insureds. Additionally, insurers may sponsor MMA training programs and/or events.

We will be pleased to provide you additional information about our compensation and information about alternative quotes upon your request. For more detailed information about the forms of compensation we receive please refer to our Marsh & McLennan Agency Compensation Guide at https://www.marshmma.com/resource/compensation-guide-for-client.pdf.

MMA's aggregate liability arising out of or relating to any services on your account shall not exceed ten million dollars ($10,000,000), and in no event shall we be liable for any indirect, special, incidental, consequential or punitive damages or for any lost profits or other economic loss arising out of or relating to such services. In addition, you agree to waive your right to a jury trial in any action or legal proceeding arising out of or relating to such services. The foregoing limitation of liability and jury waiver shall apply to the fullest extent permitted by law.

We appreciate your business!

ADDENDUM

NOTICE:

1. THE INSURANCE POLICY THAT YOU ARE APPLYING TO PURCHASE IS BEING ISSUED BY AN INSURER THAT IS NOT LICENSED BY THE STATE OF CALIFORNIA. THESE COMPANIES ARE CALLED "NONADMITTED" OR "SURPLUS LINE" INSURERS.

2. THE INSURER IS NOT SUBJECT TO THE FINANCIAL SOLVENCY REGULATION AND ENFORCEMENT THAT APPLY TO CALIFORNIA LICENSED INSURERS.

3. THE INSURER DOES NOT PARTICIPATE IN ANY OF THE INSURANCE GUARANTEE FUNDS CREATED BY CALIFORNIA LAW. THEREFORE, THESE FUNDS WILL NOT PAY YOUR CLAIMS OR PROTECT YOUR ASSETS IF THE INSURER BECOMES INSOLVENT AND IS UNABLE TO MAKE PAYMENTS AS PROMISED.

4. THE INSURER SHOULD BE LICENSED EITHER AS A FOREIGN INSURER IN ANOTHER STATE IN THE UNITED STATES OR AS A NON-UNITED STATES (ALIEN) INSURER. YOU SHOULD ASK QUESTIONS OF YOUR INSURANCE AGENT, BROKER, OR "SURPLUS LINE" BROKER OR CONTACT THE CALIFORNIA DEPARTMENT OF INSURANCE AT THE FOLLOWING TOLL-FREE TELEPHONE NUMBER: 1-800-927-4357 OR INTERNET WEB SITE WWW.INSURANCE.CA.GOV. ASK WHETHER OR NOT THE INSURER IS LICENSED AS A FOREIGN OR NON-UNITED STATES (ALIEN) INSURER AND FOR ADDITIONAL INFORMATION ABOUT THE INSURER. YOU MAY ALSO CONTACT THE NAIC'S INTERNET WEB SITE AT WWW.NAIC.ORG.

5. FOREIGN INSURERS SHOULD BE LICENSED BY A STATE IN THE UNITED STATES AND YOU MAY CONTACT THAT STATE'S DEPARTMENT OF INSURANCE TO OBTAIN MORE INFORMATION ABOUT THAT INSURER.

6. FOR NON-UNITED STATES (ALIEN) INSURERS, THE INSURER SHOULD BE LICENSED BY A COUNTRY OUTSIDE OF THE UNITED STATES AND SHOULD BE ON THE NAIC'S INTERNATIONAL INSURERS DEPARTMENT (IID) LISTING OF

APPROVED NONADMITTED NON-UNITED STATES INSURERS. ASK YOUR AGENT, BROKER, OR "SURPLUS LINE" BROKER TO OBTAIN MORE INFORMATION ABOUT THAT INSURER.

7. CALIFORNIA MAINTAINS A LIST OF APPROVED SURPLUS LINE INSURERS. ASK YOUR AGENT OR BROKER IF THE INSURER IS ON THAT LIST, OR VIEW THAT LIST AT THE INTERNET WEB SITE OF THE CALIFORNIA DEPARTMENT OF INSURANCE: WWW.INSURANCE.CA.GOV.

8. IF YOU, AS THE APPLICANT, REQUIRED THAT THE INSURANCE POLICY YOU HAVE PURCHASED BE BOUND IMMEDIATELY, EITHER BECAUSE EXISTING COVERAGE WAS GOING TO LAPSE WITHIN TWO BUSINESS DAYS OR BECAUSE YOU WERE REQUIRED TO HAVE COVERAGE WITHIN TWO BUSINESS DAYS, AND YOU DID NOT RECEIVE THIS DISCLOSURE FORM AND A REQUEST FOR YOUR SIGNATURE UNTIL AFTER COVERAGE BECAME EFFECTIVE, YOU HAVE THE RIGHT TO CANCEL THIS POLICY WITHIN FIVE DAYS OF RECEIVING THIS DISCLOSURE. IF YOU CANCEL COVERAGE, THE PREMIUM WILL BE PRORATED AND ANY BROKER'S FEE CHARGED FOR THIS INSURANCE WILL BE RETURNED TO YOU.

Date: _____

Insured: _____

NAS insurance
16501 Ventura Blvd Suite 200 Encino, CA 91436
LIC #0677191 NASinsurance.com

Vendor Management Worksheet

Service Providers

1. Please identify all service providers that have access to or help manage your network or security systems:

Name	Reason for access	Description of Services provided to the Applicant/Extent of access	Provide indemnification under contract?
Cerner	Data Center Hosting	Cerner Corporation hosts the current electronic Medical Record. The legacy systems are all hosted in hourse	☐ Yes ☐ No
	Cloud services	NA	☐ Yes ☐ No
	Web Hosting		☐ Yes ☐ No
	Managed Security Services	NA	☐ Yes ☐ No
USBank/Instamed	Payment Processing	SFTP of payment data only.	☐ Yes ☐ No
	Data Processing	NA	☐ Yes ☐ No
	Anti-virus	NA	☐ Yes ☐ No
	Firewall	NA	☐ Yes ☐ No
	IPS/IDS		☐ Yes ☐ No
Comcast	ISP		☐ Yes ☐ No
	DLP	NA	☐ Yes ☐ No
Phoenix Health Systems	Recovery Services	Data Replication	☑ Yes ☐ No

Vendor Identification

2. Please identify all service providers that have access to your network or sensitive information:

Name	Reason for access	Description of Services provided to the Applicant/Extent of access	Provide indemnification under contract?
Cerner Corporation	Medical Record System	Full support for EHR and billing systems	☐ Yes ☐ No
Phoenix Health Systems	IT support Vendor	Complete IT Outsourcing	☑ Yes ☐ No
LTSC, Inc	Interface engineering and support	Access to clinical and financial interfaces	☑ Yes ☐ No
Healthcare Resources Group	Billing Services	Billing for clinical Services	☐ Yes ☐ No
Vituity	Billing Services	Billing for ED and Hospitalist Professional Fees	☐ Yes ☐ No
Adventist Health	Hospital Management	Management of the Hospital	☐ Yes ☐ No
WIPLFI	Business Management	Management of the District	☐ Yes ☐ No
Oxford, Corp	GL and MS4 programming	Remote end user access for queries and programming	☐ Yes ☐ No
Kings Credit	Mineral King Services		☐ Yes ☐ No
Adventist Advanced Teleradiology	Radiology Services		☐ Yes ☐ No
			☐ Yes ☐ No
			☐ Yes ☐ No

3. Have any of these companies sustained any unscheduled network outage or interruption lasting longer than 4 hours within the past three (3) years that caused the Applicant to experience an interruption in business? ☐ Yes ☑ No

I understand that the information submitted herein becomes a part of my Application and, in the event that coverage is bound, is subject to the same warranty and conditions.

This worksheet must be signed by an officer of the Applicant who is acting as the authorized representative of the person(s) and entity(ies) proposed for this insurance.

The Application must be signed by an Executive Officer.

Signature: _____ Title: _____

Date: _____

A.M. BEST RATING CLASSIFICATIONS

SECURE RATINGS:

A++	Superior
A+	Superior
A	Excellent
A-	Excellent
B++	Very Good
B+	Very Good
B	Fair
B-	Fair
C++	Marginal
C+	Marginal
C	Weak
C-	Weak
D	Poor
E	Under Regulatory Supervision
F	In Liquidation
S	Rating Suspended

FPR 9	Very Strong
FPR 8 and 7	Strong
FPR 6 and 5	Good
FPR 4	Fair
FPR 3	Marginal
FPR 2	Weak
FPR 1	Poor
NR	Not Rated
NR-1	Insufficient Data
NR-2	Insufficient Size and/or Operating Experience
NR-3	Rating Procedure Inapplicable
NR-4	Company Request
NR-5	Not Formally Followed

AFFILIATION CODES:

G	Group
P	Pooled
R	Reinstated

RATING MODIFIERS:

U	Under Review
Q	Qualified

In addition, the A.M. Best Company classifies insurers on the basis of financial size categories ranging from I (smallest) to XV (largest). In $Millions of Reported Policyholders Surplus and Conditional Reserve Funds

Class I	Up to 1
Class II	1 to 2
Class III	2 to 5
Class IV	5 to 10
Class V	10 to 25
Class VI	25 to 50
Class VII	50 to 100
Class VIII	100 to 250
Class IX	250 to 500
Class X	500 to 750
Class XI	750 to 1,000
Class XII	1,000 to 1,250
Class XIII	1,250 to 1,500
Class XIV	1,500 to 2,000
Class XV	2,000 or greater