Exhibit 7

SPECIALTY RISK PROTECTOR® APPLICATION

NOTICE: THE LIMITS OF LIABILITY AVAILABLE TO PAY JUDGMENT OR SETTLEMENTS SHALL BE REDUCED BY AMOUNTS INCURRED FOR LEGAL DEFENSE AND CLAIMS EXPENSES. FURTHER NOTE THAT AMOUNTS INCURRED FOR LEGAL DEFENSE AND CLAIMS EXPENSES SHALL BE APPLIED AGAINST THE RETENTION AMOUNT. IF A POLICY IS ISSUED, SOME COVERAGE WILL BE ON A CLAIMS-MADE AND REPORTED BASIS.

Applicant refers individually and collectively to each **Insured** proposed for this insurance. The completed information provided in this **Application** will be used to determine the **Insurance Sought**. **Insurance Sought** refers to the coverage part(s) providing coverage for the insurance coverage applied for by the **Applicant**. **Insurer** shall mean the insurer that issues the policy to the **Applicant** based on this **Application**. All other terms which appear in Bold type are used in this **Application** with the same respective meanings as they have in the Specialty Risk Protector Policy.

Notwithstanding any information provided by this **Application** or any written statement, materials or documents provided in connection herewith and incorporated by reference into this **Application**, any coverage as afforded to the **Applicant**, if given, shall be solely as set forth in the terms, conditions and exclusions of the proposed policy of insurance provided to the **Applicant**, and by no other material.

Before Continuing:

Please complete the General Information, Insurance, and Financial Information sections below. The additional sections of this **Application** which are required will be determined by the **Applicant's** responses to the Desired Coverage question within the Insurance section. If available please also provide the following:

1. Sample standard contracts and agreements (with customers and independent contractors).
2. Most recent annual financial statements (if these are not publicly available).
3. Organizational chart.
4. Loss runs for the past five (5) years and information regarding any historical loss that would have exceeded the requested retention.
5. If more space is required to fully answer any question(s), please include a separate sheet(s).

GENERAL INFORMATION:

Full Name of Applicant: UT Physicians

Mailing Address: 6410 Fannin St. Houston Suite 1500, TX 77030

Business Description: Healthcare

Applicant's Web Page(s): www.utphysicians.com

Applicant's Ownership Structure:

□ Publicly Traded □ Privately Held □ Subsidiary of Publicly Traded/Privately Held Company (please provide details below) - UTP is a 501©(3).

Name of Applicant's parent organization: ____________________

Exhibit 7

Applicant's parent organization's Total Revenue (in 000,000s - most recent full fiscal year):
□ $0 - $10 □ $10 - $100 □ $100 - $500 □ >$500

Applicant's Employee Count: Domestic: _____UT Physicians leases its employees________ Total: ______________________

Number of years the Applicant has been in business: 22 years (established in 1994)

Applicant's Contact/Risk Manager:

Name: Catherine Thompson e-mail: Catherine.R.Thompson@uth.tmc.edu

INSURANCE:

Desired Coverage:

Check each of the coverage(s) that the Applicant is seeking pursuant to this Application.

☒ Cyber Extortion	☒ Network Interruption	□ Security Failure/Privacy Event Management
□ Employed Lawyers	□ Publisher and Broadcaster	☒ Security & Privacy Liability
☒ Media Content	☒ ReputationGuard®	☒ Specialty Professional Liability (Errors & Omissions)

Please indicate the inception date, and aggregate limits requested.

Requested Inception Date: Requested Aggregate Limits: $

Current Insurance:

Please indicate which of the insurance policies noted below the Applicant has purchased during the previous 12 months.

Coverage	Insurer	Expiration Date	Limits	Retention/Deductible
Employed Lawyers			$	$
Media Liability			$	$
Network Security/Privacy Liability			$	$
Professional Liability			$	$

FINANCIAL INFORMATION:

Financial Summary: Financials are attached.

If financial statements have been attached please check here ☒ and *complete only the Projected column.*

For The Projected Fiscal Year Ended: 8/31/2016

	Prior Year:	Current Year:	Projected:
Total Revenue	$	$	$171.6M
Domestic Revenue	$	$	$-
Foreign Revenue	$	$	$ -
Net Income (Loss)	$	$	
Net Cash Flows	$	$	
Cash	$	$	
Current Liabilities	$	$	

Exhibit 7

CYBEREDGE® SECURITY & PRIVACY CONTROLS AND PROCEDURES:

*Complete this section only if the **Applicant** is applying for any of the following coverages: Security and Privacy Liability, Event Management, Network Interruption, or Cyber-Extortion*

1. i) Does the **Applicant** maintain any **Confidential Information** under their care, custody, and control or with an **Information Holder**? ☒ Yes □ No
   If 'Yes', please identify the forms of **Confidential Information** maintained in either digital or hard copy:

Forms of **Confidential information** Maintained	Maintained by **Applicant**	Maintained by **Information Holder**	Estimated Number of Records	
Personal Identifiable Information (PII)	□	□	□ 0-25K □ 25K-100K □ 100K-1M	□ 1M-3M □ 3M-5M □ Over 5M
Protected Health Information (PHI)	☒	□	□ 0-25K □ 25K-100K □ 100K-1M	□ 1M-3M ☒ 3M-5M □ Over 5M
Financial Account Information	□	□	□ 0-25K □ 25K-100K □ 100K-1M	□ 1M-3M □ 3M-5M □ Over 5M
Intellectual Property/Trade Secrets	□	□		
Other:	□	□		

   ii) If maintained by **Applicant**, please check all controls in place to manage access to **Confidential Information**:

   ☒ An information handling and labeling policy dictating what information may be collected and how information should be stored
   ☒ A data retention policy outlining when data may be disposed of appropriately
   ☒ A policy of least privilege defining who may be granted access to information
   □ A process for reviewing user access privileges on a regular basis, including when a user changes positions internally
   ☒ A process for removing access privileges upon termination before the user leaves the premises

2. i) Does the **Applicant** outsource any part of their information handling, network, computer system, or information security function? □ Yes ☒ No
   If "Yes", indicate the name of the vendor providing the service:

   □ Data Center Hosting: ____________________ □ Managed Security:____________________
   □ Data Processing: □ Alert Log Monitoring:____________________
   ____
   □ Application Service Provider: ____________________ □ Intrusion Detection:____________________

   ii) Please check all due diligence that applies before engaging with a new vendor:

   ☒ Formal assessment of the security risks associated with the vendor

   ☒ A means to assess the vendors' security posture such as SAS70, CICA Section 5970, BITS or otherwise

   ☒ Contractual provision to indemnify the organization in the event of a security failure or loss on confidential information

   iii) Does the **Applicant** have a formal process in place to verify that the services are being performed as

Exhibit 7

dictated by the contract? □ Yes ☒ No

3. Check each of the following that apply to the Applicant's information security program:

☒ A formal risk assessment methodology which includes at least an annual review of organizational risks

☒ Individual officially designated as a responsible security officer (CISO, CSO, etc...)

☒ An Information Security Policy communicating how information is protected by the organization

☒ An Acceptable Use Policy communicating appropriate use of data to users

4. Check each of the following technologies used by the Applicant:

☒ Firewalls at the perimeter of the network

☒ Firewalls in front of sensitive resources inside the network

☒ Corporate antivirus/anti-malware software

☒ Intrusion detection systems

☒ Centralized log collection and monitoring

☒ Proactive vulnerability scanning/penetration testing

☒ Physical controls preventing access to the devices themselves

5. Does the Applicant have a formal process in place to automatically push updates to all computing resources for critical updates, patches and security hot-fixes? ☒ Yes □ No

If 'No', please describe: ____________________

6. Does the Applicant have processes in place to ensure that all confidential data is encrypted?

☒ Yes □ No

If "Yes", check all of the scenarios in which data is encrypted:

☒ Data at rest □ Date in transit

☒ Data transferred to removable media (backup tape, CDs, removable hard drives, etc...)

7. Is the Applicant subject to any laws or regulations dictating information security? ☒ Yes □ No

If "Yes", check all that apply:

☒ Health Insurance Portability and Accountability Act

□ Gramm-Leach-Bliley Act

□ Sarbanes-Oxley

☒ Payment Card Industry Data Security Standard

☒ Federal Education Rights Privacy Act

□ Federal Information Security Management Act

□ Red Flags Rule

☒ Other (please describe): TAC 202, UTS165 & Health Information Technology for Economic and Clinical Health Act

If 'Yes', has the Applicant undertaken any third-party security audits and complied with all recommendations? ____________________

If 'No', please describe: No third-party security audits/Vulnerability checks by 3rd party vendor.

8. Does the Applicant have:

i) A documented Business Continuity and Disaster Recovery Plan? ☒ Yes □ No

Is 'Yes', based on formal testing, what is your proven recovery time objective for critical systems to

Exhibit 7

restore operations after a computer attack or other loss/corruption?

☐ NA - have not formally tested ☐ Less than 4 hours ☐ 5 hours to 8 hours

☐ 9 hours to 12 hours ☒ 13 hours to 24 hours ☐ More than 24 hours

ii) Formal backup processes for backing up, archiving and restoring confidential data?

☒ Yes ☐ No

If 'Yes', does the **Applicant** have formal processes in place to test backup data for integrity on a periodic basis? ☒ Yes ☐ No

iii) A Documented Incident Response Plan? ☒ Yes ☐ No

9. i) Does the **Applicant** have formal processes in place to communicate, educate and train employees on data privacy and security issues? ☒ Yes ☐ No

If 'Yes', please describe the frequency and type of training: Annual online training

i) Are employees trained on their personal liability and any potential ramifications if they aid, abet, or participate in a data breach incident involving the **Applicant**? ☒ Yes ☐ No

10. Does the **Applicant** have processes in place to ensure that all employees, third parties, contractors and vendors with potential access to confidential data receive background screening?

Check all that apply:

☒ Criminal convictions ☒ Educational background ☐ Credit check

☒ Drug testing ☒ Work history ☒ Reference check

CYBEREDGE® CLOUD COMPUTING, SYSTEM FAILURE AND WRONGFUL COLLECTION COVERAGE:

Is the Applicant requesting Could Failure, System Failure and/or Wrongful Collection Coverage?

☒ Yes ☐ No

If '*Yes*', the CYBEREDGE® CLOUD COMPUTING, SYSTEM FAILURE AND WRONGFUL COLLECTION SUPPLEMENTAL QUESTIONNAIRE IS REQUIRED.

CYBEREDGE® HISTORICAL INFORMATION:

Do not complete this section if this is a renewal application.

1. During the past five (5) years, has the **Applicant** experienced any occurrences, **Claims** or **Losses** related to a failure of security of the **Applicant's** computer system or has anyone filed suit or made a **Claim** against the **Applicant** with regard to invasion or interference with rights of privacy, wrongful disclosure of **Confidential Information** or does the **Applicant** have knowledge of a situation or circumstance which might otherwise result in a **Claim** against the **Applicant** with regard to issues related to the **Insurance Sought**?

☒ Yes ☐ No

If '*Yes*', please attach complete details: Lost unencrypted specialized laptop that was a component of a medical device (fewer than 600 patients' records were on the laptop).

It is agreed that with respect to questions 1-6 above, that if such Claim, proceeding, action, knowledge, information or involvement exists, then such Claim, proceeding or action and any Claim or action arising from such Claim, proceeding, action, knowledge, information or involvement is excluded from the proposed coverage.

REPUTATIONGUARD COVERAGE:

Exhibit 7

If the Applicant is applying for ReputationGuard Coverage with a sublimit greater than one million dollars, the ReputationGuard® SUPPLEMENTAL QUESTIONNAIRE is required.

ADDITIONAL DOCUMENTS AND INFORMATION INCORPORATED BY REFERENCE

ALL WRITTEN STATEMENTS, MATERIALS OR DOCUMENTS FURNISHED TO THE INSURER' IN CONJUNCTION WITH THIS APPLICATION, REGARDLESS OF WHETHER SUCH DOCUMENTS ARE ATTACHED TO THE POLICY, ARE HEREBY INCORPORATED BY REFERENCE INTO THIS APPLICATION AND MADE A PART HEREOF, INCLUDING WITHOUT LIMITATION ANY SUPPLEMENTAL APPLICATIONS OR QUESTIONNAIRES.
ANY SECURITY ASSESSMENT, ALL REPRESENTATIONS MADE WITH RESPECT TO ANY SECURITY ASSESSMENT, AND ALL INFORMATION CONTAINED IN OR PROVIDED BY APPLICANT WITH RESPECT TO ANY SECURITY ASSESSMENT, REGARDLESS OF WHETHER SUCH DOCUMENTS, INFORMATION OR REPRESENTATIONS ARE ATTACHED TO THE POLICY ARE HEREBY INCORPORATED BY REFERENCE INTO THIS APPLICATION AND MADE A PART HEREOF.

LEGAL NOTICE AND SIGNATURES

BEFORE YOU SIGN THIS APPLICATION, READ THESE NOTICES CAREFULLY AND DISCUSS WITH YOUR BROKER IF YOU HAVE ANY QUESTIONS.

FOR THE PURPOSES OF THIS APPLICATION, THE UNDERSIGNED DULY AUTHORIZED REPRESENTATIVE OF ALL PERSON(S) OR ENTITIES PROPOSED FOR THIS INSURANCE DECLARES THAT, TO THE BEST OF HIS/HER KNOWLEDGE AND BELIEF, AFTER REASONABLE INQUIRY, THE STATEMENTS IN THIS APPLICATION, AND IN ANY ATTACHMENTS, AR TRUE AND COMPLETE.

THE UNDERSIGNED DULY AUTHORIZED REPRESENTATIVE AGREES THAT IF THE STATEMENTS AND INFORMATION SUPPLIED ON THIS APPLICATION OR INCORPORATED BY REFERENCE CHANGES BETWEEN THE DATE OF THIS APPLICATION AND THE EFFECTIVE DATE OF THE INSURANCE, HE/SHE (UNDERSIGNED) WILL, IN ORDER FOR THE INFORMATION TO BE ACCURATE ON THE EFFECTIVE DATE OF THE INSURANCE, IMMEDIATELY NOTIFY THE INSURER (SUCH CHANGES, AND THE INSURER MAY WITHDRAW OR MODIFY ANY OUTSTANDING QUOTATIONS AND/OR AUTHORIZATIONS OR AGREEMENTS TO BIND THE INSURANCE.

SIGNING OF THIS APPLICATION DOES NOT BIND THE APPLICANT OR THE INSURER TO COMPLETE THE INSURANCE, BUT IT IS AGREED THAT THIS APPLICATION AND ANY INFORMATION INCORPORATED BY REFERENCE HERETO, SHALL BE THE BASIS OF THE CONTRACT SHOULD A POLICY BE ISSUED, AND IS INCORPORATED INTO AND IS PART OF THE POLICY.

SHOULD INSURER ISSUE A POLICY, APPLICANT AGREES THAT SUCH POLICY IS ISSUED IN RELIANCE UPON THE TRUTH OF THE STATEMENTS AND REPRESENTATIONS IN THIS APPLICATION OR INCORPORATED BY REFERENCE HEREIN. ANY MISREPRESENTATION, OMISSION, CONCEALMENT OR INCORRECT STATEMENT OF A MATERIAL FACT, IN THIS APPLICATION, INCORPORATED BY REFERENCE OR OTHERWISE, SHALL BE GROUNDS FOR THE RESCISSION OF ANY POLICY ISSUED.

NOTICE TO APPLICANTS: ANY PERSON WHO KNOWINGLY AND WITH INTENT TO DEFRAUD ANY INSURANCE COMPAN OR OTHER PERSON FILES AN APPLICATION FOR INSURANCE OR STATEMENT OF CLAIM CONTAINING ANY MATERIALLY FALSE INFORMATION OR, CONCEALS, FOR THE PURPOSE OF MISLEADING, INFORMATION CONCERNING ANY FACT MATERIAL THERETO, COMMITS A FRAUDULENT ACT, WHICH IS A CRIME AND MAY SUBJECT SUCH PERSON TO CRIMIN AND CIVIL PENALTIES.

Exhibit 7

STATE FRAUD DISCLOSURES:

NOTICE TO ARKANSAS, NEW MEXICO AND WEST VIRGINIA APPLICANTS: ANY PERSON WHO KNOWINGLY PRESENT A FALSE OR FRAUDULENT CLAIM FOR PAYMENT OF A LOSS OR BENEFIT, OR KNOWINGLY PRESENTS FALSE INFORMATION IN AN APPLICATION FOR INSURANCE IS GUILTY OF A CRIME AND MAY BE SUBJECT TO FINES AND CONFINEMENT IN PRISON.

NOTICE TO COLORADO APPLICANTS: IT IS UNLAWFUL TO KNOWINGLY PROVIDE FALSE, INCOMPLETE, OR MISLEADING FACTS OR INFORMATION TO AN INSURANCE COMPANY FOR THE PURPOSE OF DEFRAUDING OR ATTEMPTING TO DEFRAUD THE COMPANY. PENALTIES MAY INCLUDE IMPRISONMENT, FINES, DENIAL OF INSURANCE, AND CIVIL DAMAGES. ANY INSURANCE COMPANY OR AGENT OF AN INSURANCE COMPANY WHO KNOWINGLY PROVIDI FALSE, INCOMPLETE, OR MISLEADING FACTS OR INFORMATION TO A POLICYHOLDER OR CLAIMANT FOR THE PURPOS OF DEFRAUDING OR ATTEMPTING TO DEFRAUD THE POLICYHOLDER OR CLAIMANT WITH REGARD TO A SETTLEMENT OR AWARD PAYABLE FROM INSURANCE PROCEEDS SHALL BE REPORTED TO THE COLORADO DIVISION OF INSURANCE WITHIN THE DEPARTMENT OF REGULATORY AUTHORITIES.

NOTICE TO DISTRICT OF COLUMBIA APPLICANTS: WARNING: IT IS A CRIME TO PROVIDE FALSE OR MISLEADING INFORMATION TO AN INSURER FOR THE PURPOSE OF DEFRAUDING THE INSURER OR ANY OTHER PERSON. PENALTIE INCLUDE IMPRISONMENT AND/OR FINES. IN ADDITION, AN INSURER MAY DENY INSURANCE BENEFITS IF FALSE INFORMATION MATERIALLY RELATED TO A CLAIM WAS PROVIDED BY THE APPLICANT.

NOTICE TO FLORIDA APPLICANTS: ANY PERSON WHO KNOWINGLY AND WITH INTENT TO INJURE, DEFRAUD, OR DECEIVE ANY INSURER FILES A STATEMENT OF CLAIM OR AN APPLICATION CONTAINING ANY FALSE, INCOMPLETE OR MISLEADING INFORMATION IS GUILTY OF A FELONY IN THE THIRD DEGREE.

NOTICE TO KANSAS APPLICANTS: ANY PERSON WHO KNOWINGLY AND WITH INTENT TO DEFRAUD, PRESENTS, CAUSES TO BE PRESENTED OR PREPARED WITH KNOWEDLGE OR BELIEF THAT IT WILL BE PRESENTED TO OR BY AN INSURER, PURPORTED INSURER, BROKER OR ANY AGENT THEREOF, ANY WRITTEN STATEMENT AS PART OF, OR IN SUPPORT OF, AN APPLICATION FOR THE ISSUANCE OF, OR THE RATING OF AN INSURANCE POLICY FOR PERSONAL OR COMMERCIAL INSURANCE, OR A CLAIM FOR PAYMENT OR OTHER BENEFIT PURSUANT TO AN INSURANCE POLICY FOR COMMERCIAL OR PERSONAL INSURANCE WHICH SUCH PERSON KNOWS TO CONTAIN MATERIAL FALSE INFORMATION CONCERNING ANY FACT MATERIAL THERETO; OR CONCEALS, FOR THE PURPOSE OF MISLEADING, INFORMATION CONCERNING ANY FACT MATERIAL THERETO COMMITS A FRAUDULENT INSURANCE ACT.

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

NOTICE TO LOUISIANA APPLICANTS: ANY PERSON WHO KNOWINGLY PRESENTS A FALSE OR FRAUDULENT CLAIM FC PAYMENT OF A LOSS OR BENEFIT OR KNOWINGLY PRESENTS FALSE INFORMATION IN AN APPLICATION FOR INSURANC IS GUILTY OF A CRIME AND MAY BE SUBJECT TO FINES AND CONFINEMENT IN PRISON.

NOTICE TO MAINE APPLICANTS: IT IS A CRIME TO KNOWINGLY PROVIDE FALSE, INCOMPLETE OR MISLEADING INFORMATION TO AN INSURANCE COMPANY FOR THE PURPOSE OF DEFRAUDING THE COMPANY. PENALTIES MAY INCLUDE IMPRISONMENT, FINES OR A DENIAL OF INSURANCE BENEFITS.

NOTICE TO MARYLAND APPLICANTS: ANY PERSON WHO KNOWINGLY AND WILLFULLY PRESENTS A FALSE OR FRAUDULENT CLAIM FOR PAYMENT OF A LOSS OR BENEFIT OR WHO KNOWINGLY AND WILLFULLY PRESENTS FALSE INFORMATION IN AN APPLICATION FOR INSURANCE IS GUILTY OF A CRIME AND MAY BE SUBJECT TO FINES AND CONFINEMENT IN PRISON.

Exhibit 7

NOTICE TO MINNESOTA APPLICANTS: A PERSON WHO FILES A CLAIM WITH INTENT TO DEFRAUD OR HELPS COMMIT A FRAUD AGAINST AN INSURER IS GUILTY OF A CRIME.

NOTICE TO NEW JERSEY APPLICANTS: ANY PERSON WHO INCLUDES ANY FALSE OR MISLEADING INFORMATION ON A APPLICATION FOR AN INSURANCE POLICY IS SUBJECT TO CRIMINAL AND CIVIL PENALTIES.

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 OR STATEMENT OF CLAIM CONTAINING ANY MATERIALLY FALSE INFORMATION, OR CONCEALS FOR THE PURPOSE OF MISLEADING, INFORMATIO CONCERNING ANY FACT MATERIAL THERETO, COMMITS A FRAUDULENT INSURANCE ACT, WHICH IS A CRIME, AND SHALL ALSO BE SUBJECT TO A CIVIL PENALTY NOT TO EXCEED FIVE THOUSAND DOLLARS AND THE STATED VALUE OI THE CLAIM FOR EACH SUCH VIOLATION.

NOTICE TO OHIO APPLICANTS: ANY PERSON WHO, WITH INTENT TO DEFRAUD OR KNOWING THAT HE IS FACILITATING A FRAUD AGAINST AN INSURER, SUBMITS AN APPLICATION OR FILES A CLAIM CONTAINING A FALSE OR DECEPTIVE STATEMENT IS GUILTY OF INSURANCE FRAUD.

NOTICE TO OKLAHOMA APPLICANTS: WARNING: ANY PERSON WHO KNOWINGLY, AND WITH INTENT TO INJURE, DEFRAUD OR DECEIVE ANY INSURER, MAKES ANY CLAIM FOR THE PROCEEDS OF AN INSURANCE POLICY CONTAINING ANY FALSE, INCOMPLETE OR MISLEADING INFORMATION IS GUILTY OF A FELONY (365:15-1-10, 36 §3613.1).

NOTICE TO OREGON APPLICANTS: ANY PERSON WHO KNOWINGLY AND WITH INTENT TO DEFRAUD ANY INSURANCE COMPANY OR OTHER PERSON FILES AN APPLICATION FOR INSURANCE OR STATEMENT OF CLAIM CONTAINING ANY MATERIALLY FALSE INFORMATION OR, CONCEALS, FOR THE PURPOSE OF MISLEADING, INFORMATION CONCERNING ANY FACT MATERIAL THERETO, COMMITS A FRAUDULENT ACT, WHICH MAY BE A CRIME AND MAY SUBJECT SUCH PERSON TO CRIMINAL AND CIVIL PENALTIES.

NOTICE TO PENNSYLVANIA APPLICANTS: ANY PERSON WHO KNOWINGLY AND WITH INTENT TO DEFRAUD ANY INSURANCE COMPANY OR OTHER PERSON FILES AN APPLICATION FOR INSURANCE OR STATEMENT OF CLAIM CONTAINING ANY MATERIALLY FALSE INFORMATION OR CONCEALS FOR THE PURPOSE OF MISLEADING, INFORMATIOI CONCERNING ANY FACT MATERIAL THERETO COMMITS A FRAUDULENT INSURANCE ACT, WHICH IS A CRIME AND SUBJECTS SUCH PERSON TO CRIMINAL AND CIVIL PENALTIES.

NOTICE TO TENNESSEE, VIRGINIA AND WASHINGTON APPLICANTS: IT IS A CRIME TO KNOWINGLY PROVIDE FALSE, INCOMPLETE OR MISLEADING INFORMATION TO AN INSURANCE COMPANY FOR THE PURPOSE OF DEFRAUDING THE COMPANY. PENALTIES INCLUDE IMPRISONMENT, FINES AND DENIAL OF INSURANCE BENEFITS.

NOTICE TO VERMONT APPLICANTS: ANY PERSON WHO KNOWINGLY AND WITH INTENT TO DEFRAUD ANY INSURANC COMPANY OR OTHER PERSON FILES AN APPLICATION FOR INSURANCE OR STATEMENT OF CLAIM CONTAINING ANY MATERIALLY FALSE INFORMATION OR, CONCEALS, FOR THE PURPOSE OF MISLEADING, INFORMATION CONCERNING ANY FACT MATERIAL THERETO, COMMITS A FRAUDULENT ACT, WHICH MAY BE A CRIME AND MAY SUBJECT SUCH PERSON TO CRIMINAL AND CIVIL PENALTIES.

The undersigned is a duly authorized representative of the Applicant and hereby acknowledges that reasonable inquiry has been made to obtain the answers herein which are true, correct, and complete to his/her best knowledge and belief.

The undersigned authorized officer of the Applicant hereby acknowledges that he/she is aware that the Limit of Liability contained in this policy shall be reduced, and may be completely exhausted, by the costs of legal defense and, in such event, the Insurer shall not be liable for the costs of legal defense or for the amount of any judgment or settlement to the extent that such exceeds the Limit of Liability of this policy.

Exhibit 7

The undersigned authorized officer of the Applicant hereby further acknowledges that he/she is aware that legal defense costs that are incurred shall be applied against the retention amount.

Signed ______________________________
(Duly authorized representative, by and on behalf of the Applicant)

Date 9-12-16

Title COO UT PHYSICIANS Organization:

(Must be signed by an authorized officer) (Organization's seal)

Attest ______________________________
(Duly authorized representative, by and on behalf of the Applicant)

Producer ______________________________
License Number ______________________________
Address ______________________________
____

Exhibit 7

BEAZLEY: PAYMENT CARD TRANSACTIONS UNDERWRITING WORKSHEET

Please fully complete each question. If necessary, please use a separate sheet to provide a full response.

Full Name of Applicant: UT Physicians

1. Please describe how payment card data is captured and transferred to credit card processor:

UT Physicians has multiple methods of payment card data intake:

1. POS analog Credit Card Terminals at clinic locations.
2. Patient initiated payments taken online via 3rd party payment platform hosted by Simplificare, Inc. Product name is SimpleePay.
3. Payments are taken by our 3rd party healthcare biller at their phone center in Norcross, GA on a web based product, Global Transport. Global Transport is provided by our processor, Global Payments, Inc.

2. Are you required to adhere to the PCI Data Security Standards by a financial institution or credit card processor as a part of the Merchant Services Agreement or otherwise required to be PCI compliant through any other contractual agreement? ☒ Yes ☐ No

If "Yes":
Are you required to submit a Report on Compliance (ROC) or a Self-Assessment Questionnaire (SAQ) to document compliance with the PCI Data Security Standards? ☐ ROC ☒ SAQ ☐ Neither

3. When was your last ROC or SAQ report submitted? 10/30/15

4. Did your last SAQ or ROC indicate that you are in compliance with current PCI Data Security Standards? ☒ Yes ☐ No

Are you currently compliant with the PCI Data Security Standards version 3.0 ☒ Yes ☐ No

If "No," when do you anticipate being compliant with PCI version 3.0

5. What was the date of the last quarterly network scan completed by an Approved Scan Vendor? See attachment

Did your last quarterly network scan by an Approved Scan Vendor result in a noncompliant scan report (i.e., did the scan report any Level 5 ('Urgent'), Level 4 ('Critical'), or Level 3 ('High') vulnerabilities? ☐ Yes ☐ No SEE ATTACHMENT

If "Yes," please describe the remediation status for the identified vulnerabilities:

6. Are hardware based point-of-interaction devices being used for payment processing? ☒ Yes ☐ No

If 'Yes', please list the name and version of these device(s) here:
VeriFone 520, VeriFone 610, VeriFone 680

7. Is a 3rd party payment processing application being used? ☒ Yes ☐ No

Exhibit 7

Has the application undergone PA-DSS validation? □ Yes ☒ No

If 'No', please list the name and version of software application(s) here:

Simplee Back Office v10.1, Simplee has gone through PCI DSS.

Exhibit 7

8. Have all default and vendor supplied passwords for payment applications and POS systems been modified and are adhering to complexity requirements as required by the PCI DSS? ☒ Yes □ No

How often are such passwords updated? See attachment

9. Is cardholder data (PAN, CVV) stored or otherwise retained for any purpose after a transaction? □ Yes ☒ No

If so, For how long is card data stored in your system after a transaction?

Do you store consumer card data in your systems for future transactions? □ Yes ☒ No

10. Do you employ any of the following: tokenization or end-to-end encryption (including encryption of databases) to protect payment card data?
□ Tokenization
□ End to end encryption

11. Are all the devices, computers and servers that handle payment card transactions inside your network segmented by documented services and ports through business need by firewalls at each Internet connection as well as from the remainder of your corporate network? □ Yes □ No
SEE ATTACHMENT

Have you restricted access to and from the PCI environment to only necessary systems and ports inside your corporate environment? □ Yes □ No
SEE ATTACHMENT

Do you restrict external traffic from "untrusted" networks and hosts? □ Yes □ No
SEE ATTACHMENT

Is outbound traffic from the PCI environment restricted to specific external IP addresses? □ Yes □ No
SEE ATTACHMENT

12. Is traffic and/or activity from the PCI environment restricted to only external sources needed to maintain/update the application and network? □ Yes □ No
SEE ATTACHMENT

Please describe which external sources the PCI environment can access:

See attachment

13. Does any portion of your POS system or card processing environment utilize an unsupported operating system such as Windows XP, Windows NT or older? □ Yes ☒ No

If 'Yes," please describe all compensating controls and your plans to update operating systems:

14. Have you restricted remote administrative access to your POS systems to only allow access during active support calls? ☒ Yes □ No

15. When did you last check your POS systems for malware? See attachment

How often do you check your POS systems for malware? See attachment

Have you discovered any malware on your POS systems in the last 12 months? □ Yes □ No
SEE ATTACHMENT

16. Please describe your procedures in place to prevent physical tampering of POS terminals:
See attachment

Exhibit 7

17. A Does the organization have a vendor management program that addresses compliance with your information security policies? ☒ Yes □ No

If no, please provide details on your vendor management program:

Section II - Non-Compliance
If you are not in compliance with current PCI Data Security Standards, please complete this section. Otherwise, please skip this section.

18. Please provide a general description of the areas where you are out of compliance:

19. Please describe your remediation efforts to attain compliance with the issues noted above:

20. Please describe any compensating controls that you have implemented:

21. By what date do you plan to attain compliance?

Completed by: Jim Vitt

Title: AVP of Finance

Date: 9/23/16

Exhibit 7

ATTACHMENT FOR BEAZLEY UNDERWRITING WORKSHEET

N/A = Not Applicable

5. N/A due to environment and the requirements of SAQ B v3.1.

8. Users of the Global Transport platform are automatically forced by the product settings to change their password every 90 days.

   Passcodes for the VeriFone devices located at our clinics are changed from the original vendor supplied passwords. All terminal keypads are required to be locked at the end of the day or if left unattended. Access to terminals is restricted to only authorized personnel.

11. N/A: All POS credit card terminals transmit data either via secure analog phone lines or via a cellular network.

    The Global Transport product is utilized solely by our third party healthcare biller at their phone center in Norcross, GA. The facility is PCI compliant.

    The Simplee online patient payment system is hosted by a third party, Simplificare, Inc. and as previously noted Simplee is PCI-DSS compliant.

    All remaining questions under number 11 are N/A due to the payment environment and the requirements of SAQ B v3.1.

12. N/A due to the payment environment and the requirements of SAQ B v3.1.

15. All questions under 15 are N/A due to the payment environment and the requirements of SAQ B v3.1.

16. All clinic personnel that have access to POS terminals are required to go through Treasury training informing them that the terminals should be physically inspected daily for any signs of noticeable tampering, additions of foreign devices into or onto the equipment, or replacement by a different device. The VeriFone devices will also display a "Tamper" message if physically opened, damaged, or if jarred enough to flip and enable the internal tamper switch. If tampering is suspected, employees are instructed to stop processing payments through the device and to immediately contact UTP Clinic Admin or Treasury. In addition, clinic personnel are required to verify the identity of any personnel claiming repair or maintenance work to the terminal device. No repair or maintenance call will be made on equipment without prior arrangements coordinated by Treasury.

Exhibit 7

BEAZLEY BREACH RESPONSE

INSURING AGREEMENTS A., C., D. AND E. OF THIS POLICY PROVIDE COVERAGE ON A CLAIMS MADE AND REPORTED BASIS AND APPLY ONLY TO CLAIMS FIRST MADE AGAINST THE INSURED DURING THE POLICY PERIOD OR THE OPTIONAL EXTENSION PERIOD (IF APPLICABLE) AND REPORTED TO THE UNDERWRITERS DURING THE POLICY PERIOD OR AS OTHERWISE PROVIDED IN CLAUSE X. OF THIS POLICY. AMOUNTS INCURRED AS CLAIMS EXPENSES UNDER THIS POLICY SHALL REDUCE AND MAY EXHAUST THE LIMIT OF LIABILITY AND ARE SUBJECT TO RETENTIONS.

INSURING AGREEMENT B. OF THIS POLICY PROVIDES FIRST PARTY COVERAGE ON AN INCIDENT DISCOVERED AND REPORTED BASIS; COVERAGE UNDER THIS INSURING AGREEMENT APPLIES ONLY TO INCIDENTS FIRST DISCOVERED BY THE INSURED AND REPORTED TO THE UNDERWRITERS DURING THE POLICY PERIOD.

These Declarations along with the completed and signed **Application** and the Policy with endorsements shall constitute the contract between the **Insureds** and the Underwriters.

Underwriters: Syndicate 2623/623 at Lloyd's.

Policy Number: W1C7E6160101

Authority Reference Number: B6012BUSANMSL1601

Item 1. **Named Insured:** UT Physicians

Address: 6410 Fannin Street
Suite 1500

Houston, TX 77030

Item 2. **Policy Period:**

From: 08-Sep-2016

To: 08-Sep-2017

Both dates at 12:01 a.m. Local Time at the Address stated in Item 1.

Please refer to the Beazley Breach Response Policy in reference to the Limits and Retentions set out in these Declarations.

Item 3. A. **POLICY AGGREGATE LIMIT OF LIABILITY**

1. For all **Damages, Claims Expenses, Penalties** and **PCI Fines, Expenses and Costs**: USD $10,000,000

But sublimited to:

Exhibit 7

	2. Aggregate sublimit of liability applicable to Insuring Agreement C. (Regulatory Defense and Penalties)	USD $10,000,000
	3. Aggregate sublimit applicable to Insuring Agreement E. (PCI Fines, Expenses and Costs):	USD $10,000,000
	B. **LIMITS OF COVERAGE FOR PRIVACY BREACH RESPONSE SERVICES:**	
	1. **Notified Individuals** Limit of Coverage: A sublimit of up to 10% of the **Notified Individuals** Limit of Coverage applies to **Notified Individuals** residing outside of the United States, which amount is part of and not in addition to the **Notified Individuals** Limit of Coverage	2,000,000 **Notified Individuals** in the aggregate
	2. Aggregate Limit of Coverage for all **Computer Expert Services**, **Legal Services** and **Public Relations and Crisis Management Expenses** combined:	USD $2,500,000

Coverage for all **Privacy Breach Response Services** is separate from and in addition to the **Policy Aggregate Limit of Liability.**

Item 4.	**RETENTIONS**:	
	A. Each **Claim Retention**:	USD $100,000
	B. **Privacy Breach Response Services** Threshold and Retention:	
	1. **Notification Services**, **Call Center Services**, and **Breach Resolution and Mitigation Services** for each incident involving at least:	100 **Notified Individuals**
	2. **Retention** applicable to **Computer Expert Services**, **Legal Services** and **Public Relations and Crisis Management Expenses**:	USD $10,000 combined, but USD 5,000 for **Legal Services** (which retention is part of and not in addition to the combined retention)
Item 5.	**Premium**: (plus applicable taxes and fees)	
Item 6.	**Retroactive Date:**	Full Prior Acts
Item 7.	**Optional Extension Period:**	
	(a) Premium for Optional Extension Period:	100% of the premium for the Policy
	(b) Length of Optional Extension Period:	12 Months

Exhibit 7

Item 8. **Continuity Date:** 08-Sep-2016

Item 9. **Notification under this Policy:**

(a) Claims:
Beazley Group
Attn: TMB Claims Group
1270 Avenue of the Americas, 12th Floor
New York, NY 10020
Email: bbr.claims@beazley.com

(b) Privacy Breaches under Insuring Agreement B.:
Email: bbr.claims@beazley.com
Toll-Free 24-Hour Hotline: (866) 567-8570
(Emails and call reports from the toll-free hotline are forwarded to the Breach Response Services Team for response)

(c) All other notices under this Policy shall be given to:
Beazley USA Services, Inc.
30 Batterson Park Road
Farmington, CT 06032
Te: (860) 677-3700
Fax: (860) 679-0247
(All Claims and Privacy Breaches must be reported in accordance with 9.(a) and 9.(b) above)

Item 10. **Service of process in any suit shall be made upon:**

Mendes & Mount, LLP
750 7th Ave # 24
New York, NY 10019

Item 11. **Choice of Law:** New York

Item 12. **Endorsements Effective At Inception:**

1.	SCHEDULE2016	Lloyd's Security Schedule 2016
2.	NMA1256	Nuclear Incident Exclusion Clause-Liability-Direct (Broad) (U.S.A.)
3.	NMA1477	Radioactive Contamination Exclusion Clause-Liability-Direct (U.S.A.)
4.	E02804 032011 ed.	Sanction Limitation and Exclusion Clause
5.	E06800 052016 ed.	Fraudulent Instruction Coverage
6.	A01110TX 022014 ed.	Important Notice
7.	E06606 122014 ed.	Telecommunications Fraud Endorsement
8.	E06571 032015 ed.	Amend Exclusion T. - Cyber Terrorism
9.	E02226 082010 ed.	Amend Consent and Settlement Clause
10.	E03409 122011 ed.	Optional Extension Period Amendment

Exhibit 7

11	E07411 052016 ed. .	First Party Computer Security Coverage Endorsement

Dated: 30-Sep-2016

At: 30 Batterson Park Road
Farmington
Connecticut 06032
(the office of the Correspondent)

By

Beazley USA Services, Inc.
(Correspondent)