



Broker: _____ Contact person _____
 _____ email _____
 _____ Phone _____

FFacts Cyber / Regulatory Medical Billing Application

The insurance for which you are applying is a claims-made and reported form of coverage. Only claims first made and reported to the Underwriters on or after the effective date but before the end of the Policy Period, or any applicable extended reporting period, will be covered, subject to any retroactive date.

This Application will give the Underwriters an understanding of your Data Breach practices. The completion of this application does not bind coverage. **All questions must be answered completely.** If a question is not applicable, answer by stating "Not Applicable" or "NA". If the answer to a question is none, answer by indicating "None" or "O". If more space is needed to answer a question, attach a separate piece of paper and identify the question to which it pertains. **The Warranty Statement (Section VIII) must be completed and signed by an officer of the practice.**

Section I – General Information

- 1) Applicant Name _____
 Address _____

 Phone _____ Email _____
 Date business established ____ / ____ / ____ Website _____
- 2) Application type individual corporation partnership other (*describe*) _____
- 3) Proposed Effective date ____ / ____ / ____ Proposed Retro date ____ / ____ / ____
- 4) Do you currently have Regulatory (billing errors) or Data Breach insurance in place? Yes No
 a) If yes please provide
 Carrier _____ Limits _____ Retention _____

Section II – Business Operations

- 5) Nature of Operations (physician group, hospital or other) _____
- | | |
|--|--------------------|
| 6) List all subsidiaries and other locations | Ownership Interest |
| _____ | _____ % |
| _____ | _____ % |
- 7) Total patient records stored electronically? _____ (Estimate)
- 8) Total # of physician(s) _____ Full time _____ Part Time _____ Employees
(for physician groups, please attach roster)

Section IV – Data Security

- 21) Is all confidential data that is stored and transmitted within and from your organization encrypted? Yes No
If no, what measures are in force to protect the network and data?

- 22) Do you store personal client information on laptops and other portable devices? Yes No N/A
If yes, is encryption in place? Yes No
- 23) Does your security policy include mandated training for all employees? Yes No
- 24) Do you process, store or handle credit card payments? Yes No N/A
a) If yes, are you PCI-DSS Compliant? Yes No
b) What % of your annual transactions is performed by credit cards? _____
- 25) Other than factory default settings, do you have regularly updated antivirus software and firewalls in place? Yes No
- 26) Do you have regularly updated antivirus software and firewalls in place within your network and undertake offsite data back-ups on at least a monthly basis? Yes No
- 27) Does the applicant carry out an IT security audit and implement all recommendations within the suggested time frame? Yes No
- 28) Has the applicant ever had a wire transfer, telecom fraud or phishing-attack loss? Yes No
If yes, please provide facts surrounding the matter on separate paper including actions implemented to avoid recurrence.
- 29) Do you require two parties to sign off on any payment transfers greater than \$2,000? Yes No
- 30) Do you have a policy in place to verify any changes to existing invoices, bank deposit Information, and contact information? Yes No

Section V - Third Party Service Providers

- 31) Identify Third Party Service providers providing the following services. *(If none please indicate)*
- a) Internet Service _____
(Internet browsing)
- b) Security Services _____
(Anti Virus)
- c) Web Hosting _____
(Your web page or portal hosting service)
- d) ASP Services _____
(Application Service Providers / external management systems)
- e) Data Processing _____
(Any other third party provider handling your data)
- f) Point of Sale _____
(Credit / Debit card or other payment processing service)

Section VI – Loss History

32) During the last 5 years, have you or anyone else in the organization:

- a) Do you have any knowledge of an action that may result in a claim? Yes No
- b) Been reviewed by a State Board of Medical Examiners? Yes No N/A
- c) Been audited or investigated by Medicaid/Medicare billing practices Yes No N/A
- d) Been audited or investigated by any local, state or federal agencies regarding health care services provided or reimbursement thereof? Yes No N/A
- e) Been investigated for anti-kickback issues? Yes No N/A
- f) Ever had a deselection action or lawsuit made by a commercial payor? Yes No N/A

If you answered “yes” to any part of Q#21, please provide the facts including final outcome on a separate piece of paper.

Section VIII – Warranty

The Undersigned warrants and represents that, to the best of his/her knowledge, the statements herein are true, and that reasonable efforts have been made to obtain sufficient information to facilitate the proper and accurate completion of this Application. It is represented that the particulars and statements contained in the Application, and any materials submitted (which shall be on file with the Underwriters) are the basis for the proposed insurance and are to be considered incorporated into and constituting a part of the proposed insurance.

The Undersigned agrees that in the event this Application contains misrepresentations or fails to state facts materially affecting the risk assumed by the Underwriters, any insurance issued shall be void in its entirety.

The Undersigned agrees that, if after the date of this Application and prior to issuance of any insurance, any occurrence, event or other circumstance should render any of the information contained in this Application inaccurate or incomplete, the Undersigned shall notify the Underwriters of such occurrence, event or circumstance, and shall provide the Underwriters with information that would complete, update or correct the information contained in this Application. Any outstanding quotations may be modified or withdrawn at the sole discretion of the Underwriters.

The Underwriters are hereby authorized to make an investigation and inquiry in connection with this application as it may deem necessary.

The Undersigned warrants that they are duly authorized by the by laws of the group or entity to execute this warranty on behalf of the group or entity, and confirms that they have made the necessary inquiries to assure underwriters of the accuracy of the statements made hereon.

Signature of Officer/Owner

Title

Print name

Date

Insurance Company Ratings & Admitted Status

Underwriters at Lloyd's London A XV Non-Admitted

If the above indicated coverage is placed with a Non-Admitted Carrier, the carrier is doing business in the state as a surplus lines or non-admitted carrier. As such, this carrier is not subject to the same regulations which apply to an admitted carrier nor do they participate in any insurance guarantee fund applicable in that state.

*The above A.M. Best Rating was verified on the date the proposal document was created.

Guide to Best Ratings

Rating Levels and Categories

LEVEL	CATEGORY	FINANCIAL SIZE CATEGORIES			
		(In \$000 of Reported Policyholders' Surplus Plus Conditional Reserve Funds)			
A++, A+	Superior				
A, A-	Excellent	FSC I	Up to 1,000	FSC IX	250,000 to 500,000
B++, B+	Good	FSC II	1,000 to 2,000	FSC X	500,000 to 750,000
B, B-	Fair	FSC III	2,000 to 5,000	FSC XI	750,000 to 1,000,000
C++, C+	Marginal	FSC IV	5,000 to 10,000	FSC XII	1,000,000 to 1,250,000
C, C-	Weak	FSC V	10,000 to 25,000	FSC XIII	1,250,000 to 1,500,000
D	Poor	FSC VI	25,000 to 50,000	FSC XIV	1,500,000 to 2,000,000
E	Under Regulatory Supervision	FSC VII	50,000 to 100,000	FSC XV	2,000,000 or more
F	In Liquidation	FSC VIII	100,000 to 250,000		
S	Suspended				

Best's Insurance Reports, published annually by A.M. Best Company, Inc., presents comprehensive reports on the financial position, history, and transactions of insurance companies operating in the United States and Canada. Companies licensed to do business in the United States are assigned a Best's Rating which attempts to measure the comparative position of the company or association against industry averages. A Best's Financial Strength Rating opinion addresses the relative ability of an insurer to meet its ongoing insurance obligations. It is not a warranty of a company's financial strength and ability to meet its obligations to policyholders.

View the A.M. Best Important Notice: Best's Credit Ratings for a disclaimer notice and complete details at <http://www.ambest.com/ratings/notice>. Best's Credit Ratings are under continuous review and subject to change and/or affirmation. For the latest Best's Credit Ratings and Best Credit Reports (which include Best Ratings), visit the A.M. Best website at <http://www.ambest.com>.

See Guide to Best's Credit Ratings for explanation of use and charges. Copies of the Best's Insurance Reports for carriers listed above are also available upon request of your Boynton & Boynton representative. Best's Credit Ratings reproduced herein appear under license from A.M. Best and do not constitute, either expressly or impliedly, an endorsement of (Licensee's publication or service) or its recommendations, formulas, criteria or comparisons to any other ratings, rating scales or rating organizations which are published or referenced herein. A.M. Best is not responsible for transcription errors made in presenting Best's Credit Ratings. Best's Credit Ratings are proprietary and may not be reproduced or distributed without the express written permission of A.M. Best Company.

Boynton & Boynton companies use A.M. Best Company's rating services to evaluate the financial condition of insurers whose policies we propose to deliver. Boynton & Boynton companies make no representations and warranties concerning the solvency of any carrier, nor does it make any representation or warranty concerning the rating of the carrier which may change.



As an adjunct of your policy with Boynton Healthcare, your company now has access to the **eRiskHub**[®], powered by NetDiligence[®].

The eRiskHub is a private web-based portal containing information and technical resources that can assist you in the prevention of network, cyber and privacy losses and support you in the timely reporting and recovery of losses if an incident occurs.

The eRiskHub portal is an internet-based service that features news, content and services from leading practitioners in risk management, computer forensics, forensic accounting, crisis communications, legal counsel, and other highly-specialized segments of cyber risk.

Please note the following:

1. The eRiskHub portal is a private site for customers of Boynton Healthcare only. Do not share portal access instructions with anyone outside your organization. You are responsible for maintaining the confidentiality of the **Access Code** provided to you.
2. Up to three individuals from your organization may register and use the portal. Ideal candidates include your company's Risk Manager, Compliance Manager, Privacy Officer, IT Operations Manager or Legal Counsel.
3. This portal contains a directory of experienced providers of cyber risk management and breach recovery services. Boynton Healthcare does not endorse these companies or their respective services. Before you engage any of these companies, we urge you to conduct your own due diligence to ensure the companies and their services meet your needs. Unless otherwise indicated or approved, payment for services provided by these companies is your responsibility.
4. Should you experience a data breach event, you may choose to call one of the Breach Coaches listed in the portal for immediate triage assistance. Your initial consultation of up to one half-hour is free of charge. Please be aware that the Breach Coach[®] service is provided by a third-party law firm. Therefore, contacting a Breach Coach does NOT satisfy the claim notification requirements of your policy.

To register for the Boynton Healthcare eRiskHub:

1. Go to <https://www.eriskhub.com/ffacts>
2. Complete the **New User Registration** form in the center of the webpage. Create your own Username and password. Enter **08663-450** in the **Access Code** field.
3. Once you've completed registration, you can login immediately by entering the Username and password you just created in the **Login** box in the top right corner of the screen.



ACCORDING TO THE IDENTITY THEFT RESOURCE CENTER (ITRC), A RECORD HIGH **1,093 BREACHES** EXPOSING MORE THAN **36 MILLION RECORDS** OCCURRED IN 2016.

When a breach event occurs, time is of the essence. Having a breach response plan in place with access to the third-party resources you need can help you efficiently and cost-effectively respond to and recover from the breach.

As a Boynton Healthcare policyholder, you will receive complimentary access to the eRiskHub® portal, powered by NetDiligence®. Boynton Healthcare eRiskHub provides tools and resources to help you understand your exposures, establish a response plan and minimize the effects of a breach on your organization.

Key Features of the eRiskHub Portal

- **Incident Roadmap** – includes suggested steps to take following a network or data breach incident, free consultation with a BreachCoach® and access to a breach response team
- **News Center** – cyber risk stories, security and compliance blogs, security news, risk management events and helpful industry links
- **Learning Center** – best-practices articles, white papers and webinars from leading technical and legal practitioners
- **Risk Manager Tools** – assists you in managing your cyber risk including a self-assessment and state breach notification laws
- **eRisk Resources** – a directory to quickly find external resources with expertise in pre- and post-breach disciplines



The eRiskHub® portal is an effective way to help you combat cyber losses with minimal, controlled and predictable costs.

**FOR MORE INFORMATION ABOUT BOYNTON HEALTHCARE AND
THE eRISKHUB®, CONTACT US TODAY AT
FFACTS@BOYNTONANDBOYNTON.COM!**