FFActs
Healthcare Compliance Insurance

Broker: _____ Contact person _____

_____ email _____

_____ Phone_____

FFActs Regulatory Medical Billing/Cyber Liability and Breach Response 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.

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 V) 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 Regulatory (billing errors) or Data Breach insurance in Place? ☐ Yes ☐ No

a) If yes please provide

Regulatory Carrier_____ _____ _____ Limits_____ Retention_____

Cyber 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 # of physician(s) _____ Full time _____Part Time _____Employees
(for physician groups, please attach roster)

Section III – Operations and Financial Information

8) Payor Information:

Payer Source	Gross Billings (past 12 months)	Net Collections (past 12 months)
Medicare	$	$
Medicaid	$	$
Commercial	$	$
Other	$	$
TOTAL	$	$

9) Net revenues

_____ _____ _____

Last year *Current year* *Next year*

***Please include most recent financials (audited preferred)**

10) Do you have a process in place for resolving disputes with clients? ☐ Yes ☐ No

11) Do you have a billing compliance program? ☐ Yes ☐ No

12) Is there a written policy regarding the collection of receivables? ☐ Yes ☐ No

13) Does your organization use a CPT manual when billing? ☐ Yes ☐ No

14) Are all contracts and referral relationships reviewed by outside counsel to ensure they conform with anti-kickback statutes? ☐ Yes ☐ No

15) Is billing monitored to alert management of possible up-coding or other billing anomalies? ☐ Yes ☐ No

16) Does your practice monitor free/discounted samples of medications to guard against or inappropriate billing? ☐ Yes ☐ No ☐ N/A

17) Does your organization comply with HIPAA's privacy rule? ☐ Yes ☐ No

18) Is any physician in your organization required to serve "on-call" for patients requiring emergency treatment? ☐ Yes ☐ No ☐ N/A

If yes, is the physician familiar with their responsibilities under EMTALA? ☐ Yes ☐ No

19) Is billing handled by a Third Party billing company? ☐ Yes ☐ No ☐ N/A

If yes,

a) Is there common ownership? ☐ Yes ☐ No

b) Is there a compliance program in place? ☐ Yes ☐ No

c) How many are credentialed billers? _____

Section IV – Regulatory and Medical Billing Loss History

20) 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 V – Regulatory and Medical Billing 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

FFActs
Healthcare Compliance Insurance

FFActs Cyber Liability and Breach Response Application

This Application will give the Underwriters an understanding of your Data Breach practices. All questions must be completed to be provided a Cyber Liability and Breach Response Insurance quotation. The completion of this application does not bind coverage. The DECLARATION must be completed and signed by an officer of the practice.

PLEASE NOTE: If you do not wish to receive a quote for Cyber Liability, this section of the application does not need to be completed.

1) Does the applicant use Google G-Suite, Office 365 or other similar cloud-based infrastructure with the four network security best-practice guidelines listed in Question 2 enabled? ***(if yes, continue to Question 4).*** ☐ Yes ☐ No
   If no, please provide brief details of what measures are in force to protect such information
   _____

2) Which of the following security best-practice guidelines does the applicant have enabled on its network(s):
   - 2.1 Filtering all incoming emails and communications for malicious links, spam, malware and attachments. ☐ Yes ☐ No
   - 2.2 Multi-factor Authentication for all user account ☐ Yes ☐ No
   - 2.3 Sender Policy Framework ☐ Yes ☐ No
   - 2.4 Advanced Threat Protection settings (if no, answer below) ☐ Yes ☐ No
     - 2.4.1 Does this applicant use AWS Security Hubs? ☐ Yes ☐ No
     - 2.4.2 Please provide full details of compensatory controls

     _____

3) Does the applicant have the following protocols in place:
   - 3.1 All system configuration and data is either (i) subject to regular back-ups at least weekly via secure cloud or (ii) maintained in office copies disconnected from the organization's network? ☐ Yes ☐ No
   - 3.2 Multi-factor Authentication settings are enabled for access to back-up files? ☐ Yes ☐ No
   - 3.3 Data is encrypted in all cases while it is in transit, at rest and on portable devices? ☐ Yes ☐ No

4) Does the applicant have processes in place to implement, within 14 days, critical security, anti-virus and malware patches received from commercial software vendors onto all of its servers, laptops, desktops, routers, firewalls, phones and other physical devices? (if no, answer below) ☐ Yes ☐ No
   - 4.1 Within how many days are critical security, anti-virus and malware patches received from commercial software vendors implemented on physical devices? Number of days: _____

5) Does the applicant provide all employees with anti-fraud training at least annually? ☐ Yes ☐ No
(including but not limited to detecting social engineering, phishing training, business email compromise and other similar exposures)
   - 5.1 Before processing funds transferred and/or third-party account detail changes, applicant confirms the transaction details with the requestor, through a secondary means of communication*? ☐ Yes ☐ No
   - 5.2 Do you require two parties to sign off on any payment transfers greater than $5,000? ☐ Yes ☐ No

*A secondary means of communication is different from the first means of communication. For example, if the request is received by telephone, a secondary communication may be an email.

6) Do you process store or handle credit card payments and are you PCI-CSS Compliant? ☐ Yes ☐ No

THIRD PARTY SERVICE PROVIDERS (Contact your IT department or vendor for guidance)

7) 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 services)

8) Within the last five (5) years, has the applicant suffered any systems intrusions, tampering, virus or malicious code attacks, loss of data, loss of portable media, hacking incidents, extortion attempts, data theft, cyber data breach incident, wire transfer crime incident, telecom fraud or phishing attack loss resulting that would be covered by this insurance? ☐ Yes ☐ No

If "Yes", please provide facts surrounding the matter on a separate paper including actions implemented to avoid reoccurrence.

CYBER LIABILITY AND BREACH RESPONSE DECLARATION (must be completed and signed by an officer)
On behalf of the applicant, I declare that the applicant has made a fair presentation of the risk, by disclosing all material maters which the applicant knows or ought to know or, failing that, by giving the insurer sufficient information to put a prudent insurer on notice that it needs to make further inquiries in order to reveal material circumstances. In addition, the applicant acknowledges that the data it discloses to the insurer may be transferred outside of the European Economic Area.

_____ _____
Signature of Applicant Position/Title

_____ _____
Print Name Date

Signed on behalf of the applicant by: _____