eHealth

Insurance application form

UK

The purpose of this application form is for us to find out more about you. You must provide us with all information which may be material to the cover you wish to purchase and which may influence our decision whether to insure you, what cover we offer you or the premium we charge you.

How to complete this form

The individual who completes this application form should be a senior member of staff at the company and should ensure that they have checked with other senior managers and colleagues responsible for arranging the insurance that the questions are answered accurately and as completely as possible. Once completed, please return this form to your insurance broker.

Section 1: Company Details

1.1 Please state the name and address of the principal company for whom this insurance is required. Cover is also provided for the subsidiaries of the principal company, but only if you include the data from all of these subsidiaries in your answers to all of the questions in this form.

Legal entity name:

Company name:

Primary address (address, county, postcode, country):

Website:

1.2 Date the business was established (DD/MM/YYYY):

1.3 Number of employees: Employee Reference No. (ERN):

1.4 Please confirm your current wage roll: £

1.5 Please state your gross revenue in respect of the following years:

	Last complete financial year	Estimate for current financial year	Estimate for next financial year
Domestic revenue:	£	£	£
USA revenue:	£	£	£
Total gross revenue:	£	£	£
Profit (Loss):	£	£	£

1.6 Date of company financial year end (DD/MM/YYYY):

Please provide details for the primary contact for this insurance policy:

Contact name: Position:

Email address: Telephone number:

CFC Underwriting Limited is Authorised and Regulated by the Financial Conduct Authority

Section 2: Activities

2.1 Please describe in detail 1) the nature and types of professional and/or technology services you are engaged in and 2) the types of technology products developed, manufactured, licensed or sold:

2.2 Please state whether your technology services are used for diagnosis, treatment or prevention of diseases or other conditions? □ Yes □ No

2.3 Please provide an approximate breakdown of how your revenue is generated from your products and services:

	%
	%
	%
	%
	%
	%
	%
	%

2.4 Please indicate the estimated number of patient encounters for the next 12 months:

2.5 Please confirm the percentage of your consultations which are are peer-reviewed by a Chief Medical Officer or equivalent? %

(If you have a quality assurance process, then please provide a copy)

2.6 Please state whether all professionals are subject to background checks (criminal, sexual offender registry etc.): □ Yes □ No

If "no", please provide details:

2.7 Please state whether any doctor has had a board action brought against them in the last 5 years: □ Yes □ No

If "yes", please provide details:

2.8 Please state whether medications are prescribed through your services: □ Yes □ No

Section 3: Contract & Risk Management Information

3.1 Please complete the following in respect of your 3 largest projects in the past 3 years:

Name of client:	Nature of your work undertaken:	Your annual income from this contract:	Duration:

3.2 Please state approximately how many customers you have:

3.3 Please state whether you always carry out work under a written contract signed by every client: □ Yes □ No

3.4 Please describe how, if at all, you limit your liability for consequential loss or financial damages under a written contract:

3.5 Please describe your legal review process, if any, before entering into new contracts or agreements:

3.6 Please describe the impact on your clients if your products or services failed or you were unable to deliver your products or services:

3.7 Do you employ subcontractors? □ Yes □ No

If "yes", please state:

a) what approximate percentage of your revenue, in your current financial year, will be paid to subcontractors (%):

b) whether you sign reciprocal hold harmless agreements: □ Yes □ No

c) whether you ensure that subcontractors have their own errors and omissions and general liability insurance: □ Yes □ No

d) if you answered "yes" to c) above, what is the limit of liability that subcontractors must purchase:

Section 4: Cyber Security Risk Management

Please complete the following details for the entire company or group (including all subsidiaries) that is applying for the insurance policy. Any defined terms will be bolded and highlighted in blue and can be found in the glossary at the end of this application form:

4.1 IT infrastructure and resourcing

Please confirm the name of your **managed service provider** (if applicable):	
What is the approximate number of servers on your network?	
What is the approximate number of desktops and laptops on your network?	
What is your annual IT budget?	
What approximate percentage of your IT budget is spent on IT security?	

Is any part of your IT infrastructure outsourced to third party technology providers, including application service providers? □ Yes □ No

If you answered "yes" to the question above, please list your critical third party technology providers below (up to a maximum of 10), including a brief summary of the technology services they provide for you:

4.2 Please provide the approximate number of unique individuals that you collect, store and/or process personally identifiable information from, whether on your own systems or with third parties:

□ 0-50,000 □ 50,001-100,000 □ 100,001-250,000 □ 250,001-500,000

□ 500,000+ *If in excess of 500,000 records, please confirm the exact amount:*

Please confirm full details on this data, including the type and nature.

4.3 Please describe your approach towards protecting sensitive and confidential information (e.g. access controls, encryption, network segmentation etc.):

4.4 Please describe details of how often you purge records that are no longer required:

4.5 Please state whether you are compliant with the Data Protection Act AND EU General Data Protection Regulation (GDPR) AND any applicable health data protection regulation in the relevant countries where services are provided to and in: □ Yes □ No

4.6 Please confirm whether multi-factor authentication is required for *all remote access to your network*: □ Yes □ No

If you use an alternative method for securing remote access to your network, such as certificate based authentication for devices, please provide details here:

4.7 Please confirm whether multi-factor authentication is required to access *all cloud resources holding sensitive or confidential information*: □ Yes □ No

4.8 Please describe what detection capabilities you have to alert you to malicious activity within your environment. Please include details of any endpoint detection and network monitoring tools used.

4.9 Please describe your patch management process and how you ensure that all critical patches are applied in a timely fashion, including a timeframe of how quickly you would implement patches for zero day vulnerabilities after they have been released by the vendor:

4.10 Please describe your data back-up policy in detail, including how the back-ups are stored (e.g. online, offline, cloud storage etc.), how frequently your back-ups are taken, how you secure your back-ups, how you test your back-ups and how regularly you test them, and how many back-ups copies you take:

4.11 Please tick all the boxes below that relate to controls that you currently have implemented within your IT infrastructure (including where provided by a third party). If you're unsure of what any of these tools are, please refer to the explanations on the final page of this document.

□ Application whitelisting
□ Asset inventory
□ Custom threat intelligence
□ Database encryption
□ Data loss prevention
□ DDoS Mitigation
□ DMARC
□ DNS Filtering
□ Employee awareness training
□ Endpoint detection & response
□ Incident response plan
□ Intrusion detection system
□ Next-generation firewalls
□ Penetration testing
□ Perimeter firewalls
□ Security operations centre (SOC)
□ Virtual private network (VPN)
□ Vulnerability scanning
□ Web application firewall
□ Web content filtering

Please provide the name of the software or service provider that you use for each of the controls highlighted above:

Section 5: Intellectual Property Rights Risk Management

5.1 Please describe below your procedures for:

a) preventing infringing on third party intellectual property rights; and

b) obtaining licenses to use and the monitoring of third party intellectual property rights:

5.2 Please state whether you have ever sent or received the following relating to intellectual property rights:

a) a cease and desist letter: □ Yes □ No

b) notification of an actual or potential claim letter: □ Yes □ No

If "yes" to a) or b) above, please provide full details:

5.3 Please describe your procedures for managing intellectual property rights issues, including responding to an allegation of infringement and how the individual responsible for intellectual property rights issues is qualified for the role:

Section 6: Claims Experience

6.1 Please state whether you are aware of any incident:

a) which may result in a claim under any of the insurance for which you are applying to purchase in this application form: □ Yes □ No

b) which resulted in legal action being made against any of the companies to be insured within the last 5 years: □ Yes □ No

If you have answered "yes" to a) or b) above then please describe the incident, including the monetary amount of the potential claim or the monetary amount of any claim paid or reserved for payment by you or by an insurer. Please include all relevant dates, including a description of the status of any current claim which has been made but has not been settled or otherwise resolved.

Section 7: Additional Information

Please provide the following information when you send the application form to us.
- Directors or principals resumes if the company has been trading for less than 3 years;
- The organisation chart or group structure if any subsidiaries are to be insured including names, dates of acquisition, countries of domicile, percentages of ownership; and
- The standard form of contract, end user license agreement or terms of use issued by the company.

Name:	Date of Acquisition:	Country of Domicile:	Percentage of ownership:

Please provide this space below to provide us with any other relevant information:

Important notice

*By signing this form you agree that the information provided is both accurate and complete and that you have made all reasonable attempts to ensure this is the case by asking the appropriate people within your business. CFC Underwriting will use this information solely for the purposes of providing insurance services and may share your data with third parties in order to do this. We may also use anonymised elements of your data for the analysis of industry trends and to provide benchmarking data. For full details on our privacy policy please visit **www.cfcunderwriting.com/privacy***

Contact Name: Position:

Signature: Date (DD/MM/YYYY):

cfc

Glossary of terms

UK

Application whitelisting

A security solution that allows organisations to specify what software is allowed to run on their systems, in order to prevent any nonwhitelisted processes or applications from running.

Asset inventory

A list of all IT hardware and devices an entity owns, operates or manages. Such lists are typically used to assess the data being held and security measures in place on all devices.

Custom threat intelligence

The collection and analysis of data from open source intelligence (OSINT) and dark web sources to provide organisations with intelligence on cyber threats and cyber threat actors pertinent to them.

Database encryption

Where sensitive data is encrypted while it is stored in databases. If implemented correctly, this can stop malicious actors from being able to read sensitive data if they gain access to a database.

Data loss preventions

Software that can identify if sensitive data is being exfiltrated from a network or computer system.

DDoS mitigation

Hardware or cloud based solutions used to filter out malicious traffic associated with a DDoS attack, while allowing legitimate users to continue to access an entity's website or web-based services.

DMARC

An internet protocol used to combat email spoofing – a technique used by hackers in phishing campaigns.

DNS filtering

A specific technique to block access to known bad IP addresses by users on your network.

Employee awareness

Training programmes designed to increase employees' security awareness. For example, programmes can focus on how to identify potential phishing emails.

Endpoint protection

Software installed on individual computers (endpoints) that uses behavioural and signature based analysis to identify and stop malware infections.

Incident response plan

Action plans for dealing with cyber incidents to help guide an organisation's decision-making process and return it to a normal operating state as quickly as possible.

Intrusion detection system

A security solution that monitors activity on computer systems or networks and generates alerts when signs of compromise by malicious actors are detected.

Managed service provider

A third party organisation that provides a range of IT services, including networking, infrastructure and IT security, as well as technical support and IT administration.

Multi-factor authentication

Where a user authenticates themselves through two different means when remotely logging into a computer system or web based service. Typically a password and a passcode generated by a physical token device or software are used as the two factors.

Network monitoring

A system, utilising software, hardware or a combination of the two, that constantly monitors an organisation's network for performance and security issues.

Penetration tests

Authorized simulated attacks against an organisation to test its cyber security defences. May also be referred to as ethical hacking or red team exercises.

Perimeter firewalls

Hardware solutions used to control and monitor network traffic between two points according to predefined parameters.

Vulnerability scans

Automated tests designed to probe computer systems or networks for the presence of known vulnerabilities that would allow malicious actors to gain access to a system.

Web application firewall

Protects web facing servers and the applications they run from intrusion or malicious use by inspecting and blocking harmful requests and malicious internet traffic.

Web content filtering

The filtering of certain web pages or web services that are deemed to pose a potential security threat to an organisation. For example, known malicious websites are typically blocked through some form of web content filtering.

CFC Underwriting Limited is Authorized and Regulated by the Financial Conduct Authority