eHealth

Insurance application form

REST OF WORLD

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, state, postcode, country):

Website:

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

1.3 Number of employees:

1.4 Please state which currency you are reporting in:

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):			

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

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

Contact name: Position:

Email address: Telephone number:

Section 2: Activities

2.1 [illegible] professional, healthcare and/or [illegible]

2.2 [illegible] [illegible] [illegible]

2.3 Please state whether you are involved with the provision of any tangible products, including the manufacture, (re)packaging, (re)labelling or distribution: [illegible] [illegible]

If "yes", please provide details:

2.4 [illegible]

	[illegible]
	[illegible]
	[illegible]
	[illegible]
	[illegible]
	[illegible]
	[illegible]
	[illegible]

2.5 [illegible]

2.6 [illegible]

[illegible]

2.7 [illegible] [illegible] [illegible]

[illegible]

2.8 [illegible] state whether any doctor has been subject to disciplinary proceedings or sanctions by a medical regulatory authority (such as the Irish Medical Council) within the past 5 years: [illegible] [illegible]

If "yes", please provide details:

2.9 [illegible] [illegible] [illegible]

2.10 Please state whether you prescribe any controlled substances: ☐ ĥŇr ☐ ¸ ɐ

If "yes", please provide details:

Section 3: Contract & Risk Management Information

3.1 ƚďŇĂrŇ Qɐ ʙ ŋďŇʌŇ ʌ ţ Ň ŘɐďɐΞ ďʌ r ďʌ ŒŇr ŋŇQʌ ɐŘ ʳ ɐ ʔ ǝ ᵉ ďĂǝ r Ňr ʌ ŋǝɐŸŇQʌ r ďʌ ʌ ţ Ň ŋĂr ʌ ᵉ ʳŇĂǝr ī

¸ Ă ʙ Ň ɐŘ QďŇʌʌī	¸ Ăʌ ʔ ǝŇ ɐŘ ʳ ɐ ʔ ǝ Ξ ɐǝȶ ʔ ʌ ǳŇǝʌĂȶŇʌī	ĥ ɐ ʔ ǝ ĂʌʌʔĂďʌQɐ ʙ Ň Řǝɐ ʙ ʌ ţ ďr QɐʌǝĂQʌī	Ε ʔ ǝĂ ďɐʌī

3.2 ƚďŇĂrŇ r ʌĂʌŇ Ăŋŋǝɐ ï ď ʙ ĂʌŇ ʳ ţ ɐ Ξ ʙ Ăʌ ʳ Q ʔ r ʌɐ ʙ Ňǝr ʳ ɐ ʔ ţ ĂŴŇī

3.3 ƚďŇĂrŇ r ʌĂʌŇ Ξ ţ Ňʌ ţ Ňǝ ʳ ɐ ʔ ĂďΞ Ă ʳ r QĂǝǝ ʳ ɐ ʔ ʌ Ξ ɐǝȶ ʔ ʌ ǳŇǝ Ă Ξ ǝďʌʌŇʌ QɐʌǝĂQʌ r ď r ʌŇ ǳ ǩ ʳ ŇŴŇǝ ʳ QďŇʌʌī ☐ ĥŇr ☐ ¸ ɐ

3.4 ƚďŇĂrŇ ǳŇr Qǝď ǩŇ ţ ɐ Ξ ʳ ďŘ Ăʌ ĂďŘ ʳ ɐ ʔ ď ʙ ďʌ ʳ ɐ ʔ ǝ ďĂǩďďʌ ʳ Řǝɐ Qɐʌ r Ň ǝ ʔ Ňʌ ďĂďɐ r r ɐǝ Řďʌ Ă ʌ QďĂďǳ Ă ʙ Ă r Ňr ʔ ʌ ǳ Ňǝ Ă Ξ ǝďʌʌŇʌ QɐʌǝĂQʌī

3.5 ƚďŇĂrŇ state the standard and maximum liability caps you agree in contracts:

3.6 ƚďŇĂrŇ ǳŇr Qǝď ǩŇ ʳ ɐ ʔ ǝ ďŇ r Ăď ǝŇŴ ďŇ Ξ ŋǝɐQŇr r ďŘ Ăʌ ʳ ǩŇŘɐǝŇ ŇʌʌŇǝďʌ r ďʌɐ ʌŇ Ξ QɐʌǝĂQʌ ɐǝ Ă r ǝŇŇ ʙ Ňʌʌī

3.7 ƚďŇĂrŇ ǳŇr Qǝď ǩŇ ʌ ţ Ň ď ʙ ŋĂQʌ ɐʌ ʳ ɐ ʔ ǝ QďŇʌʌ ďŘ ʳ ɐ ʔ ǝ ŋǝɐǳ ʔ Qʌ ɐǝ r Ňǝ ŴďQŇ r Řďďʌ ǳ ɐǝ ʳ ɐ ʔ Ξ ŇŇ ʔ ʌĂǩďŇ ʌɐ ǳŇďď ŴŇǝ ʳ ɐ ʔ ǝ ŋǝɐǳ ʔ Qʌ ɐǝ r ŇǝŴ ďQŇ r ī

3.8 Ε ɐ ʳ ɐ ʔ Ň ʙ ŋďɐ ʳ r ʔ ǩ Qɐʌʌ ǝĂQʌɐǝ r Š ☐ ĥŇr ☐ ¸ ɐ

ďŘ ʳ Ňr ʳ ŋďŇĂrŇ r ʌĂʌŇ:

Ăų Ξ ţ Ăʌ Ăŋŋǝɐ ï ď ʙ ĂʌŇ ŋŇǝQŇʌʌĂ r Ň ɐŘ ʳ ɐ ʔ ǝ ǝŇŴŇʌ ʔ Ň ď r ʌ ʔ ǝʌŇǝŇǳ ʌ ţ ǝɐ ʔ r ţ ǩ Ň ŋĂďǳ ʌɐ r ʔ ǩ Qɐʌʌ ǝĂQʌɐǝ r ųųį

ǩų Ξ ţ Ňʌ ţ Ňǝ ʳ ɐ ʔ r ď r ʌ ǝŇQɐǝǳ ŋǝɐŴďǳ ŇǳĂďďʌ ɐŘ ď ďʌ ʌ ţ Ăʌ ʙ ďɐ r r Ă r ǝŇŇ ʙ Ňʌ r ī ☐ ĥŇr ☐ ¸ ɐ

Qų Ξ ţ Ňʌ ţ Ňǝ ʳ ɐ ʔ ǝŇ ʔ ʔ ďǝŇ ʌ ţ Ăʌ r ʔ ǩ Qɐʌʌ ǝĂQʌɐǝ r ţ ĂŴŇ ʌ ţ Ňďǝ ɐ Ξ ʌ professional indemnity/medical malpractice aʌǳ r ŇʌŇǝĂď ďďĂǩďďďʌ ʳ ďʌr ʔ ǝĂʌQŇī ☐ ĥŇr ☐ ¸ ɐ

ǳų ďŘ ʳ ɐ ʔ Ăʌ r Ξ Ňǝ Ňǳ Ẋ ʳ Ňr Ẍ ʌɐ Qų Ăǩɐ ŴŇ Ξ ţ Ăʌ ďr ʌ ţ Ň ď ʙ ďʌ ɐŘ ďďĂǩďďďʌ ʳ ʌ ţ Ăʌ r ʔ ǩ Qɐʌʌ ǝĂQʌɐǝ r ʙ ʔ r ʌ ŋ ʔ ǝQ ţ Ă r Ňī

eHealth

Insurance application form

REST OF WORLD

Section 4: Cyber Security Risk Management

[illegible]

4.1 IT infrastructure and resourcing

[illegible] managed service provider [illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

4.2

[illegible]

[illegible]

4.3

[illegible]

4.4 æﾑÑĂrÑ ǅÑrǪœʠĶÑ ǅÑʌĂʠﾑr ɐȒ ţɐ꞊ ɐȒʌÑɅ ʳɐʔ ɳʔœȓÑ œÑǪɐœǅr ʌţĂʌ ĂœÑ Ʌɐ ﾑɐɅ ȓÑœ œÑɵʔʠœÑǅr̄

4.5 Please state whether you are compliant with the Irish Data Protection Act 2018, the 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 that multi-factor authentication is always enabled on all of your email accounts: ☐ Yes ☐ No

---

4.7 æﾑÑĂrÑ ǪɐɅȒʠœ Ƀ ꞊ ţÑʌţÑœ multi-factor authentication ʠr œÑɵʔʠœÑǅ Ȓɐœ *all remote access to your network*: ☐ ĥÑr ☐ ¸ɐ

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

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

---

4.9 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.

4.10 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:

4.11 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:

4.12 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:

4.13 Please confirm that **before** any change is made to a third party's account details, you obtain authorisation from the third party via an authentication method which is different to the original method used to request the change: ☐ Yes ☐ No

4.14 Please confirm that **before** you transfer funds to an account that you haven't paid into before, you obtain authorisation from the recipient of the funds via an authentication method which is different to the original method used to request the transfer: ☐ Yes ☐ No

4.15 Do you provide training on phishing/social engineering scams for all employees involved in transferring funds on behalf of your organisation? ☐ Yes ☐ No

If "yes", please provide details of the training you provide:

4.16 Please confirm whether you provide all clients with a written warning that if they receive a request via email to make a change to any of their account details and/or to transfer any funds that they **must not** respond to the email and that they **must** contact you immediately: ☐ Yes ☐ No

4.17 Please provide details of your Crime policy (if purchased) including limit, deductible and insurance carrier:

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

c) which has resulted in any action from a medical or healthcare regulatory authority in the past 5 years: ☐ Yes ☐ No

If you have answered "yes" to a), b) or c) 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.cfc.com***

Contact Name: Position:

Signature: Date (DD/MM/YYYY):

Glossary of terms

REST OF WORLD

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.