

Provider Registration Form

UK Healthcare Practitioners

In order for us to consider your request to become a recognised UK provider with Healix Health Services, please complete the form below. You can complete most of the information electronically, but you will need to print and sign before returning to us. Please email your completed form to UKProviderNetworkTeam@healix.com.

Once the information has been considered for recognition, you will be advised of the outcome in writing. If successful we will advise on which date your recognition becomes effective together with your unique account code.

|  |
| --- |
| 1. **Provider details**
 |
| Title: |  |
| First Name: |  |
| Surname: |  |
| Gender:*Please mark box that applies* | Female: |  | Male: |  | Other: |  |
| Billing/Correspondence Address: |  |
| Postcode: |  |
| Email address: |  |
| Telephone Number: |  |

|  |
| --- |
| 1. **Secretary Details**
 |
| Title: |  |
| Full Name: |  |
| Email Address: |  |
| Telephone Number: |  |

|  |
| --- |
| 1. **Specialty**
 |
| Is the consultant/provider a specialist or anaesthetist?*Please mark box that applies* | Consultant Specialist: |  | Consultant Anaesthetist: |  |
| What is the consultant’s/provider’s specialty? |  |
| What is the consultant’s/provider’s sub-specialty? |  |
| Does the consultant/provider treat children?*Please mark box that applies* | Yes: |  | No: |  |
| What age ranges does the consultant/provider treat?*Please mark box that applies* | 0-3 | 4-12 | 13-18 | 19-64 | 65+ |
| Use this space for any further comments/notes |  |

|  |
| --- |
| 1. **Qualifications, Details of Registration and Insurance**

*Please provide a copy of your registration certificate with this form* |
| What is your professional/regulatory body? |  |
| What is your current registration number? |  |
| Do you have personal/professional indemnity cover?*Please mark box that applies* | Yes: |  | No: |  |

|  |
| --- |
| 1. **Fees**
 |
| Will you adhere to the Healix Fee Schedule?This can be viewed at <http://hsp.healix.com/hfs> *Please mark box that applies* | Yes: |  | No: |  |
| If you do not adhere, please advise which CCSD codes you typically bill and advise your fee for those codes. | Code | Fee |
| Initial Consultation | £ |
| Follow-Up | £ |
|  | £ |
|  | £ |
|  | £ |
|  | £ |
|  | £ |
|  | £ |

|  |
| --- |
| 1. **Practicing Privileges**

*Please state all hospitals or facilities where you hold practice privileges* |
| Hospital/Practice Name | Hospital/Practice Address |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

|  |
| --- |
| 1. **Billing**

*All providers are requested to bill Healix electronically via Healthcode. For more information about electronic billing please contact Healthcode on 0330 900 4900 or visit* [*https://www.healthcode.co.uk/medical-billing/ebilling-for-providers*](https://www.healthcode.co.uk/medical-billing/ebilling-for-providers)*Alternatively invoices can be emailed to HHSInvoices@healix.com* |
| Confirm that billing will be made via Healthcode:*Please mark box that applies* | Yes: |  | No: |  |
| *NB: It is important that you submit invoices promptly as invoices submitted after a period of 6 (six) months from the date of treatment will be rejected. If this happens, you agree not to contact the patient for payment.* |

|  |
| --- |
| 1. **Bank Details**

*Payment will be made via BACS* |
| Bank Name: |  |
| Account Name: |  |
| Sort Code: |  | Account Number: |  |
| Remittance Email: |  |

|  |
| --- |
| 1. **Information Security and Data Protection**

*When providing services, personal data will be exchanged between Healix and yourself/your company such as identification information and health information. To demonstrate compliance with applicable data protection legislation, please complete this table providing as much information as possible.* |
| Please confirm that you agree to the Data Processing Agreement in Appendix 1?*Please mark box that applies* | Yes: |  | No: |  |
| Please confirm that your email domain is TLS enabled?*Please mark box that applies* | Yes: |  | No: |  |
| How do you ensure confidentiality is maintained by all authorised individuals? (I.e. included in contract, annual renewal of obligations, signed NDA etc.)  |  |
| Please provide a copy of your latest Data Security and Protection Toolkit (previously called the Information Governance Toolkit) Report and go to Section 10. |  |
| If you have not completed the Data Security and Protection Toolkit Report then please answer the Information Security and Data Protection questions below. |
| How do you limit access to the data to individuals with a Need to Know? (I.e. do you have access controls in place so only authorised individuals can access the data?) |  |
| Please confirm you have in place appropriate security measures to protect the data as described in Appendix 1, 4.4. Security Measures? *(If you are ISO27001 Certified then please provide a copy of the certificate)* | Yes: |  | No: |  |
| How do you store the data? *(On-site, Cloud based solution, Paper based?)* |  |
| In which countries is the data stored? Where is the data accessed? *(I.e. Worldwide or countries where you operate? Please provide list of countries if possible.)* |  |
| How long do you keep the data? Please confirm that all data will be securely deleted when the retention period has exceeded? |  |
| Who do you share the data with? *(Please provide categories such as ground ambulance companies etc. Please provide details if you share the data for any other purpose than to provide the services)* |  |

|  |
| --- |
| 1. **Declaration**
 |
| **Data Protection**In order to deal with your request for registration and to meet our obligations under the General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA); we would be grateful if you would complete the following declaration:I confirm my consent to the use and processing of personal details, including sensitive data, by the data controllers and relevant third parties for the following purposes:* Registration of my services with the data controllers:
* Associated administration, including but not limited to policy and claims administration
* Fraud prevention
* Payment for my services
* Enquiries into my professional practice in connection with my registration.

The Data Controller is Healix Health Services Limited. Please follow this link for further information on how we protect your personal data: <https://healix.com/provider-privacy-notice/>I will inform Healix Health Services immediately if my employment with the NHS or any other employer is suspended or terminated for whatever reason and/or if my GMC/or appropriate governing bodies’ registration is changed for whatever reason. I will inform Healix Health Services should any of the details submitted on this form change.**Terms and Conditions**By submitting your request for registration, you agree to adhere to the Practitioner Terms and Conditions. They can be found at the below link:https://healix-group.files.svdcdn.com/production/files/2023/Healix\_Practitioner\_Terms\_Conditions.pdf?dm=1695204929 |
| Signed |  |
| Date |  |
| Name (BLOCK CAPITALS) |  |

Appendix 1: Data Processing Agreement

1. For the purposes of this Agreement both Parties will be acting as Data Controllers for Personal Data and Sensitive Personal Data collected and processed when providing the Services.
2. Any terms used in this Agreement, relating to data protection, where not otherwise defined in this Agreement shall have the meanings attributed to them in applicable Data Protection Legislation.
3. This Agreement relates specifically to the General Data Protection Regulation (GDPR) that apply to all private and public organisations processing personal data for residents of the European Economic Area.
4. In the course of the provision of services there is a requirement to share Personal Data between the Parties. When sharing and processing personal data the following obligations will apply:
	1. **General Responsibilities**

The Parties, in the performance of this Agreement, comply at all times with the Data Protection Legislation and shall not perform their obligations in such a way as to cause either Party to breach any of its obligations under the Data Protection Legislation:

* Where relevant; provide a fair processing notice or obtain valid consent to ensure that the transfer has a legal basis and processing is fair and transparent where applicable:
* Have adequate records of processing activities including use and processing of personal data;
* Not share the personal data with anyone other than those with whom it is necessary for the provision of the service;
* Ensure that anyone accessing the personal data within their organisation is subject to appropriate confidentiality obligations;
* On an ongoing basis, each Party ensures that the personal data is:
	+ adequate, relevant and limited to what is necessary in relation to the purpose for which it was collected; and
	+ accurate and, where necessary, up to date having taking every reasonable step to ensure that any inaccurate personal data, has been erased or rectified.

**4.2 Data Breach**

In the event of a data breach the Parties must handle it reasonably, taking into account the interests of both Parties, and in accordance with the Data Protection Legislation. The Parties must inform each other of a relevant data breach without undue delay and no later than 24 hours after becoming aware of the data breach.

The notification must include sufficient information about the data breach and any mitigating actions taken for the other Party to assess the severity of the data breach, the risk posed to data subjects, the appropriateness of the steps being taken to remedy the data breach, mitigate any risk arising out of it and prevent it recurring, and the likelihood of any further data breaches.

If required and reasonable the Parties will work together as required to minimise the impact, perform mitigating actions and put in place mitigating controls as soon as possible.

The Parties will fully indemnify and hold the other Party harmless from and against any and all losses, damages, claims, costs and expenses suffered or incurred by or awarded against the other Party as a result of or in connection with the Party’s breach of the Data Protection Legislation.

**4.3 Subject Access Request**

The Parties shall deal with all enquiries, requests, complaints and investigations (other than in relation to a data breach) by Data Subjects or any Regulators in relation to the data that has been shared. Should any such enquiry be received by the other Party, that Party shall without undue delay (and no later than 3 working days) forward that enquiry to the other Party where relevant. The other Party will support the resolution of the request as needed.

**4.4 Security Measures**

The Parties shall provide sufficient adequate protection of the Personal Data in respect of technical and organisational security measures. The Parties must ensure that the security measures are appropriate to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected, having regard to the state of the art and the cost of their implementation.

**4.5 Sub-contracting**

In the event of sub-contracting of the processing of Personal Data in accordance with this Agreement, the processing activity must be carried out by a sub-contractor, acting on the instructions of the Data Controller of such Personal Data and providing at least the same level of protection for such Personal Data and the rights of the data subject as the Data Controller.

**4.6 International Data Transfer**

Where a Party exports Personal Data outside the EEA the data exporter shall and shall procure that sub-contractors or third parties acting on the data exporter's behalf who are processing Personal Data comply at all times with the Data Protection Legislation and shall not perform its or their obligations under the Agreement in such a way as to cause the Parties hereto to breach any of their respective obligations under the Data Protection Legislation.