UK Facility Request for Registration

In order for us to consider your request to become a recognised UK facility provider with Healix Health Services, please print & complete the form below. Your completed form can be faxed to us on 0208 481 7761 or emailed to HHSUKProviderNetworkTeam@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	
Name of Facility:	
Address:	
Post Code:	
Website address:	
Email address:	
Telephone Number:	

2. Facility information	
Brief description of available facilities or services provided:	
Please list the specialties that are provided at your facility:	

3. Regulatory information	
Is your facility registered with the CQC? If yes please provide your unique reference number.	
Name and contact details of the Responsible Officer	

4. Clinical Governance	
Please provide details of medical cover if patients stay overnight:	
What emergency transfer arrangements are in place for patients	
Do you have a practice privileges process with an active MAC?	
If not, who decides who can practice at the facility and deals with individuals clinical performance?	
Who is responsible for dealing with complaints?	

5. Tariff	
Do you currently have an agreed tariff in place with Healix Health Services?	
If no, please attach a tariff of fees for consideration. **Note**: Healix will not consider any new request for recognition unless a tariff of fees has been agreed	

6. Bank details

All payments will be made by BACS

Bank Name:	
Sort Code:	
Account Number:	
Account Name:	
Email address for remittance advice:	

7. Billing

All providers are requested to bill Healix electronically via Healthcode. For more information about electronic billing please contact Healthcode on 01784 263150 or visit ebilling.healthcode.co.uk

Confirm that billing will be made via Healthcode:	Yes:		No:	

Please note - 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.

8. Information Security and Data Protection

When providing services, personal data will be exchanged between Healix and 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?	**Yes / No**
Please confirm that your email domain is TLS enabled?	**Yes / No**
How do you ensure Confidentiality is maintained by all authorized 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. 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 authorized 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** **ISO27001 Certificate:**
How do you store the data? (On-site, Cloud based solution, Paper based?)	

In which country(ies) 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?	**Yes / No**
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?	

9. Signatory

I will inform Healix Health Services immediately if our regulatory status or registration changes or should any of the details submitted on this form change.

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. **DATA SHARING**

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.

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:

3.1 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.

3.2 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.

3.3 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.

3.4 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.

3.5 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.

3.6 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.