

Information > Carelink Hosting Environment



Introduction

Carelink Hosting is a set of services which offer high quality, secure hosting capabilities for the NHS, its partners and 3rd party software providers.

The key feature that differentiates the Carelink from other hosting services is its dual connectivity - the infrastructure is connected to both NHSnet and the Internet and this allows our customers to serve content and applications to both networks from a single location.

We are able to provide this service because the Carelink environment has been independently audited and approved by the NHSIA for a 3rd party code of connection to NHSnet. This will naturally migrate to the N3 network as this is rolled out.

Carelink is the health business of ioko and provides a range of services to in excess of 200 organisations. The vast majority of these are NHS bodies, ranging from GP's surgeries to Ambulance Trusts, PCTs to Strategic Health Authorities.

A smaller number of our customers are private sector organisations who have developed health related applications and want to make them reliably available to the NHS community on NHSnet.

Hosting Location

The Carelink infrastructure is hosted in London Dockland's Telehouse.

Telehouse is a purpose built facility providing resilient and secure IT hosting. It is widely acknowledged as the best IT hosting facility available. The state of the art control centre in the building provide up to the minute information on all requirements/operational equipment within the facility.

Hosting Security

Security of equipment is paramount to us. Telehouse is manned 24/7 by an establishment of trained Security / Operations

staff to provide a deterrent to unauthorized access. CCTV, with digital data storage space, both internally and externally provides information to a security control centre on possible intrusion. Advanced proximity access control systems prevent unauthorised access to areas within the facility.

Access Control

Proximity cards control access to the Telehouse site. These are programmed to allow access only to the necessary areas. Only authorised personnel will be granted access to the facility.

Access is monitored by security staff and historical data recorded to provide audit trails if required.

Power

Sustainable power supplies are essential to the continuous operation of equipment.

Power continuity is a prime objective of Telehouse. It has a sophisticated power distribution system for resilience. Multiple mains electricity feeds are supported by a UPS (uninterruptible power supply) system with generator backup.

All of power back-up systems are individually maintained and checked on a routine basis. Redundant n+1 equipment provides spare capacity to enable maintenance and repairs without interruption to services.

Optimum Operating Conditions

Business critical IT equipment depends on specialist facilities management. Telehouse has more experience than any other neutral co-location facility in Europe to supply the optimal operating conditions for customer equipment.

Telehouse facilities operate computerised building management systems that monitor and remotely operate sensors covering electrical, mechanical, fire detection and water leakage systems.

Telehouse provide state of the art facilities enabling customers to have complete confidence even when they cannot be present.

Key Benefits

- World Class hosting environment ensures **physical and online security** for all types of data and applications
- **Redundancy and failover** is built into the environment architecture in order to provide continuity of service
- Security staff onsite 24x7, with **roving security patrols** in addition to staff guarding building entries
- Access to the data centre is strictly **controlled to prevent forced or covert entry** into the facility
- High-density, motion-sensing digital colour **closed-circuit television cameras** (CCTV) throughout the facility
- Motion detectors and alarm systems are located throughout the facility, with a silent alarm and **automatic notification of appropriate law enforcement** officials protecting all exterior entrances
- Class 3 and **Class 4** building standards
- **Redundant bandwidth** **burstable**
- The Carelink infrastructure has been **independently audited**, to satisfy the guidelines for code of connection for the provision of web-hosting as stipulated by the NHSIA.
- Layered **NHSIA compliant firewalls**

Head Office
Innovation Close
York Science Park
York
YO10 5ZD
UK

London Office
17c Curzon Street
London
W1J 5HR
UK

t: +44 (0) 1904 438 000
f: +44 (0) 1904 435 450

e: info@ioko365.com

The Service

Support

Carelink support services are provided by a dedicated team of engineers, who have an intimate understanding of the systems and services that we provide.

Our engineers spend their time addressing and responding to customer incidents and carrying out proactive maintenance tasks on Carelink servers.

All of our servers are supported by a back-to-back contract with our hardware provider. This ensures that, in the unlikely event of a hardware failure, the fastest possible response times are implemented and faulty equipment is replaced with minimum service disruption.

The core networking infrastructure, including switches and firewalls, and every server hosted in the Carelink Environment is monitored around the clock. Server monitoring includes network connection, http response, processor usage, disk space usage as well as key processes and services. Any reported problems detected by the monitoring systems are investigated by an ioko engineer.

Our entire infrastructure is monitored 24/7 and any alerts are assigned to our engineers through our Service Desk. The Service Desk uses HP OpenView software which provides a platform for compliance with the ITIL (IT Infrastructure Library) framework.

ITIL was created by the UK government via the CCTA and is rapidly being adopted globally as the standard for best practice in the provision of IT Service.

ITIL covers a number of areas, but its main focus is on IT Service Management (ITSM). IT Service Management (ITSM) itself is generally divided into two main areas, Service Support and Service Delivery. Together, these two areas consist of 10 disciplines that are responsible for the provision and management of effective IT services.

Our adoption of the ITIL framework enables us to report and review our response times to issue resolution against our SLAs. This assists us in our ongoing endeavour to improve the service that we deliver to our customers.

Resilience and DR

Wherever possible we ensure that the Carelink infrastructure has built in resilience. This is always balanced with trying to ensure that we minimise the cost of the service to our customers.

Our Internet connection, firewalls, routers and power supplies all have levels of resiliency that ensure service continuity, or fast recovery, in the event of component failure.

Backup and Disaster Recovery

A daily incremental and weekly full back up to tape is taken of the file system and registry of every server that is hosted in the Carelink environment. These tapes are then, from the first week in any month, stored on a secure off-site facility for the period of six months.

In addition to this an image of each server is taken prior to installation, and refreshed on a regular basis.

In case of absolute disaster we aim to be able to restore a server, and all data, up to the last available back up to tape, onto suitable alternative hardware, even at an alternative location should this prove necessary.

Security

Infrastructure

The Carelink infrastructure has been independently audited, to satisfy the guidelines for code of connection for the provision of web-hosting as stipulated by the NHSIA.

Our firewalls' rules base ensures that only specified types of traffic are allowed between our hosting facility and NHSnet. They have been designed, with NHSIA approval, specifically to maintain the integrity of NHSnet and connected

organisations, and at the same time to provide a flexible platform from which health organisations can deliver content and functionality.

Staff

As a company we look after IT systems for many customers in both the public and private sectors. Many of our customers' systems contain sensitive information and maintaining the integrity of this information is something that we take very seriously.

Individual customers will often take steps to put in place appropriate levels of security within their own systems and we recognise the importance of complimenting this by proper control of access to customers' machines by our own staff.

To this end, we have an active security policy in place and access to computer systems, communications services and electronically held information is strictly limited to those staff having an authorised business requirement for such access.

Management, contractors and staff who do not comply with the security policies and procedures contained within the security policy, or who knowingly or negligently allow staff under their supervision to do so, are liable to disciplinary action, including dismissal.

What Next?

If you would like any further information on our services, please contact us on:

Web: www.carelink.co.uk

Or you can contact us directly by email, telephone or mail at the address above:

Email: info@carelink.com

Tel: 01904 438000

and ask for Carelink Sales

