

Whzan Service Definition Document – G Cloud 15

Service definition document

The Whzan software platform is a pathway agnostic, location independent and customisable Technology Enabled Care solution for monitoring, recording and assessing single/multiple patient vital signs and clinical condition. Patients can be provided with a combination of medical devices and assessments to monitor their condition(s) dictated by their clinical pathway. Whzan has already integrated over 40 Bluetooth instruments, supports manual entry for non-Bluetooth devices, and we integrate new devices and create new assessments upon request to align to the required pathway. The only requirements for users/patients/clinicians are a web browser and internet access. Clinicians can add, move or remove patients from caseloads via the Whzan dashboard therefore the supplier does not need to be involved in patient onboarding, management and offboarding.

We also provide home activity and environment monitoring devices via Whzan Guardian to support person centred care. For example, in addition to the Whzan Blue Box solution a frail or newly discharged hospital patient may require activity monitoring sensors in the place they call home which will track and detect changes to their daily routine. These changes can detect deterioration and possible illness.

As part of our ISO-27001 and Cyber Essentials plus certification we maintain, annually review, and test a full disaster recovery and business continuity plan (available on request). We host on Microsoft Azure at 2 sites in England with industry leading standards for reliability and disaster recovery. We maintain a full backup solution including both georedundancy and offline storage in England. This process is regularly audited internally and PEN tested annually by accredited external auditors.

We have a rolling 30 day x 1 hour automatic backup regime in place. The Whzan database is encrypted at rest and held in Microsoft Azure. In the case of the end of contract, the client is offered a choice of encrypted secured data formats e.g. database, Excel, zipped CSV etc. Once the data has been successfully transferred and we have written confirmation that it all can be read, we will delete the data from our database. Our second separately geolocated backup database will automatically synchronise.

We also have a secondary backup system where weekly copies of the Whzan database are made and stored in Microsoft SharePoint, these are encrypted at rest hence can only be read/accessed when moved back to the Azure platform. These weekly backups are stored on a rolling annual basis, hence after initial written deletion request it will take a year before the data is finally eliminated from all backups.

Within our healthcare application in the event of a network outage or poor signal strength, the Whzan Blue Box computer tablet stores all readings locally in an encrypted cache and transmits data to the cloud platform when connectivity is restored. This allows the tablet to cope with both short term and long-term outages, such as during a power cut or local phone cell outages. This caching is invisible to the user who can carry on using the tablet as normal.

Service availability over the last twelve months was 100.00% with a Microsoft stated average uptime of 99.98% for each hosting site.

Our support services process offers multiple access routes including helpline assistance, email, video conferencing (staffed by a team that adjusts to activity peaks), instruction documents, and web portal help videos between 9am and 5pm Monday to Friday and at other times to meet contractual requirements. Our telephone number is printed in large text on the lid of the Blue Box. For out of hours, our voicemail service records the caller's query, telephone number and name if stated. All voicemails, emails and online forms are responded to with priority the next working day. Buyers can register contact details to receive notifications and updates on significant system events.

We are regularly audited by a CREST certified third party to CHECK standards, to maintain our quality certification status for ISO 9001, ISO27001 (includes third party accredited penetration testing of Whzan), Cyber Essentials Plus (Also includes penetration testing to the same standard), and the Telecommunications Security Act. We employ a nominated security and compliance manager with direct access to senior management/board members. Our QMS allocates security responsibilities to board level.

Our Data Protection Policy explains how we meet our legal obligations concerning confidentiality and data security standards. The requirements within the policy are primarily based upon the UK General Data Protection Regulation (UK GDPR), the key legislation covering data security and confidentiality of personal and sensitive personal data in the United Kingdom.

We complete CREST standard annual penetration tests, and our Data Protection Officer will provide the reports to the Trust within 1 working day from request.

Under guidance from Solcom Management and Quality Manager, all Solcom staff ensure software is current and security patches installed without delay. Antivirus software is active on all systems and configured to automatically update regular basis. All network devices connected are protected by the company hardware firewalls configured in a NAT configuration, with additional configurations in place to detect common denial of service attacks.

External connections to the Solcom network are only allowed via the hardware VPN, each member of staff requiring access to the network is given their own Username and password independent to a User's Windows credentials.

Solcom staff abide by password policies, detailing what to avoid, suggestions for password selection, password storage, current security best practices, and advice for compromised passwords.

We operate a clear desk policy to protect sensitive corporate and client data by limiting exposure.