kinseed

Service Definition

MEDIWORK - PRODUCT AND TECHNICAL SECURITY INFORMATION

Table of Contents

Introduction **3**
About this document 3
Legal notices 3

PRODUCT, TECHNICAL & SECURITY SPECIFICATION **4**
What is MediWork 4
General Architecture and hosting 5
Security of web applications, databases, systems and information 6
Protection of Confidentiality and Integrity of Information 6
Data Security 6
Vulnerability Scans 7
Application Security Controls 7
Logical Access Restrictions 7
User Management 7
Definition of Roles by User Type 7
Data Protection during Storage 8
Facilities where data is stored 8
Sharing of Data 8
Data Export 9
Network Architecture 9
Server and Application Hardening 9
Software development lifecycle 9
Certification Held 9
Location of Servers 10
Pre and Post Engagement 10

Introduction

About this document

This document outlines the security information relating to the MediWork Platform and issued to clients when requested during implementation process.

Legal notices

This document is intended for the use of only Kinseed Limited and the above named recipients. If you believe you have received this document in error, please destroy it immediately and contact either the sender, or info@kinseed.com. Unless explicitly listed otherwise, all contents are Copyright © Kinseed Limited 2025, All Rights Reserved.

PRODUCT, TECHNICAL & SECURITY SPECIFICATION

What is MediWork

MediWork Occupational Healthcare Platform is a comprehensive, AI/ML-powered solution that enables organisations to proactively protect employee health, boost productivity, and reduce healthcare-related costs. Supported by the Department for Work and Pensions (DWP) and the Department of Health and Social Care (DHSC), MediWork transforms fragmented occupational health processes into intelligent, predictive workflows that prevent issues before they escalate.

The platform strengthens core occupational health operations through advanced booking management, automation, recall alerts, and streamlined case workflows, empowering clinicians and employers with faster decision-making, improved compliance, and measurable productivity gains.

Powered by Event Driven Architecture and AI / ML Capability

Pre-Placement – evaluating the health and fitness of individuals before they are placed in a new job or role to ensure their well-being and suitability for the position

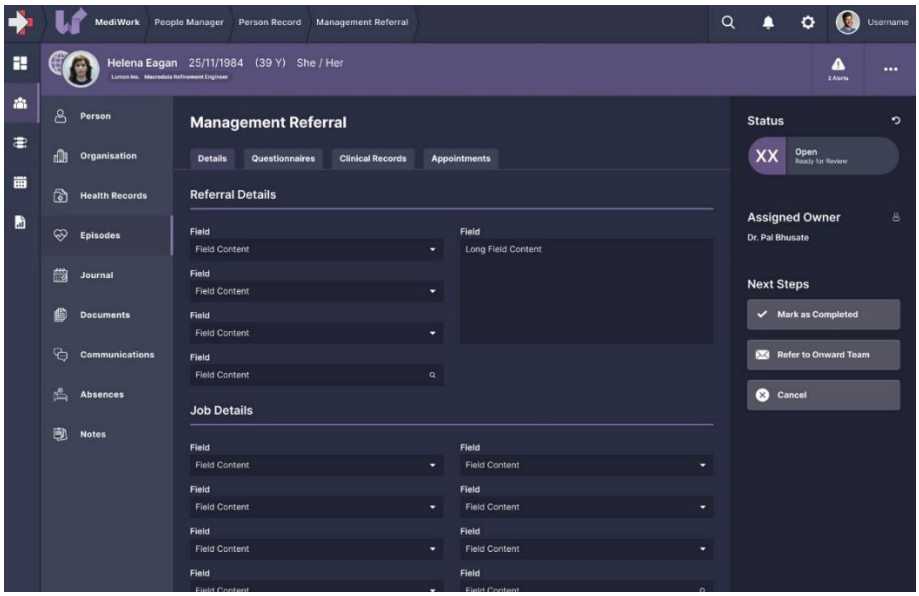
Health Surveillance - systematic process of monitoring and assessing the health of individuals in the workplace to identify and prevent work-related health risks and ensure their ongoing well-being

Case Management (incl. Sickness) - coordinated and proactive management of individual cases involving work-related illnesses, injuries, or health conditions, providing appropriate support, treatment, and interventions to promote recovery and facilitate a safe and healthy return to work

Immunization - administering vaccines to individuals in the workplace to protect them against specific infectious diseases, reducing the risk of illness and transmission among employees

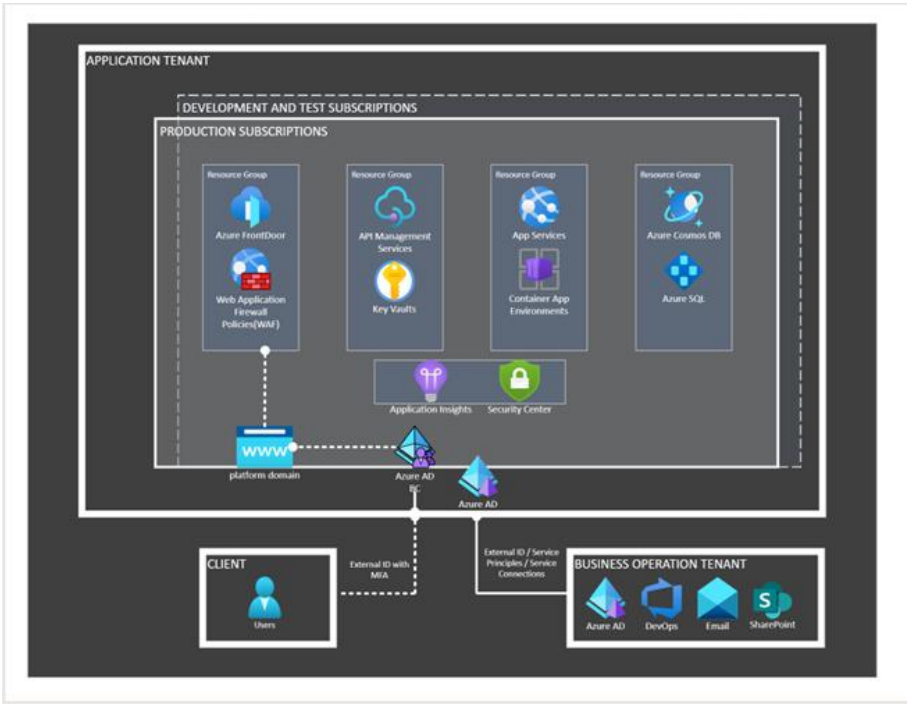
Supporting morden and intutive user experience.





General Architecture and hosting

MediWork is a specific component ("application") within MediWork, which is a cloud application hosted by Kinseed Limited. MediWork is hosted entirely within Microsoft Azure, based in Geocentrically located datacenters in the UK region. All information and processing within MediWork is conducted entirely within the UK. There are no components to MediWork which exist outside of the Microsoft Azure environment (no on-premises hardware / infrastructure, and no components within other cloud services, e.g. AWS / GCP, etc).



Security of web applications, databases, systems and information

All electronic data transfers take place over secure socket layer (SSL) connections. Every CRUD transaction within MediWork (Create, Read, Update or Delete operations) is audited permanently within the MediWork system, storing the user / account which undertook the change, which data the transaction was interacting with, and timestamps for the activities in question.

All personal data is encrypted at rest and in motion. Each user session including login is encrypted with a valid SSL certificate issued by Microsoft and Verisign with a valid SSL certificate using 256 bit encryption and a 2048 bit root/private key.

All Microsoft Azure systems are patched in real-time by Microsoft as and when vulnerabilities arise. Wherever configurable, the latest update ring is selected for Azure services, to ensure MediWork always operates on the most robust and rigid platform. Backups are taken of core data environments on a split tiered basis (high frequency backups for the past day, medium frequency backups for the past month, and low frequency backups for the past year). These backups are stored within Azure data storage elements, within the architecture laid out above.

All access to the system is managed through federated single-sign-in utilising Clients existing identity management suite (Active Directory), meaning all access controls described above in the preceding document apply to the access rights granted for the MediWork application within MediWork.

The system is architected such that the same controls are in place for Kinseed employees as are there for Client employees, ensuring that only through permission and explicit grant of rights can Kinseed employees access any part of the user data within MediWork. This ensures Kinseed as Data Processors exist as de-facto participants in the overarching Client security policy.

Protection of Confidentiality and Integrity of Information

As above, only users within Client's core identity suite are able to access MediWork – within that set of users, specifically only those licensed and approved for access are able to directly interact with the system. Each user session will automatically time out after 30 minutes of inactivity to avoid unauthorised access when a workstation is left unattended. User passwords are never stored directly in MediWork, instead relying on the robust security in place through Single-Sign-On powered through Azure Active Directory.

Data Security

Kinseed's software engineers can only access MediWork environments through a carefully monitored and configured channel, requiring the use of extremely securely configured user accounts, multi-factor authentication, and remotely managed / monitored device access. The Kinseed office has both card-access and physical key access, and their computers are fully password protected with Multi Factor Authentication and strong Azure-AD powered session attestation. Any

employee who leaves Kinseed has all access rights immediately revoked, and all live remote sessions terminated automatically,

Vulnerability Scans

Kinseed works with third party providers to undertake a full Penetration Test and Vulnerability scan on an at least annual basis. Alongside this, Kinseed utilises automated cloud app security technologies to continually scan the environment both for known vulnerabilities as they arise (removing the risk of Zero-Day exploits), and for suspicious activity (reducing the attack surface for malicious users).

Application Security Controls

Each user account accessing the system belongs to zero or more security groups, each of which grants explicit permission to perform specific operations within the system. The system is built from a "Zero Trust Basis", meaning by default the system closes all access, and a user is unable to undertake any action unless they have been explicitly granted permission to do so either directly, through their membership of a security group, or through an inherited permission of a security group's parent group.

Logical Access Restrictions

Each time a user loads a page, their credentials are checked to confirm what data they have access to and only the records owned or overseen by that user are fetched from the server. At no point does the system download or access data that the user does not have permission to see – there are no cosmetic "endpoint restricted" operations in place – the only data ever transmitted to an end user machine is data which that user is able to access.

User Management

User profile management, as it is federated from Client's own identity management system, will be handled directly within their own Active Directory system. MediWork (and MediWork as a whole) will therefore always be provided with access to the most up to date list of users and information about them.

When an account is expunged from the identity management suite (e.g. leaving user / organisation), MediWork will retain the data that user created, so as not to leave gaps in data.

Adding a new user is performed by Client Admin team, by adding the user to their internal Active Directory Identity management suite.

Definition of Roles by User Type

MediWork provides the following roles by default, but additional role groups can be generated either for Client's employees, or for those accessing MediWork / MediWork from within a client organisation:

Role	Definition
Super Administrator	Members of Kinseed Limited, who are able to do anything on the system
Administrator	Members of Client Team, who are able to do and see anything on the system
Manager / HR / Health & Safety	Members of Client Team, who are able to do all a contributor can do, but also able to approve requests or delete key clinical records.
Contributor	Members of Client Team, who are able to do all a viewer can do, but also able to create records, change their content, or configure reports to be generated.
Viewer	Members of Client Team, who are able to read data within the system, or generate pre-configured reports.

Data Protection during Storage

Online electronic data transfers take place over secure socket layer (SSL) connections. Offline data transfers for backups etc, are made over internal, non-accessible direct Azure connectivity. Personal data in the database is encrypted and the encryption keys are stored only in Azure Key Vault, which provides not only direct access as required to decryption routines, but also significantly improved logging against use of cryptographic functions, as well as automated key rotation and monitoring.

Facilities where data is stored

All data that is stored on the MediWork environment are hosted within Microsoft Azure, which is fully operated by Microsoft.

Microsoft certifications can be found at https://learn.microsoft.com/en-us/azure/compliance/ and include ISO 9001, 27001, 27017 and 27018.

Sharing of Data

Direct data transfer (database-level retrieval) is never provided to any other third party application. MediWork supports the use of secure and authenticated RESTful APIs, should Client or other Client's agent require the need to connect data to other applications. All APIs in question fully adhere to the previously outlined security standards, including for encryption, auditing, and information protection.

Data Export

MediWork supports the ability for Client to produce defined exports / reports based on the data inside the application. Any data exported through this method is only done to the level and content of data which the user is already granted access to.

There is no functionality within MediWork for Client to directly export the full database. Kinseed is available on request by Client to help export data within MediWork “in bulk”, should the need arise, but this would be performed manually as a direct interaction with data stores.

Network Architecture

Microsoft Azure platform services are highly sophisticated data storage and hosting facilities with all state-of-the art controls in place. For more information, visit azure.microsoft.com

Server and Application Hardening

All elements of MediWork (including MediWork) are only publicly accessible through “Azure Front Door”, which provides powerful firewall, anti-intrusion, anti-DOS and load balancing capabilities. Within the backend of the application, all instances of code runners and data stores are configured to select the highest dependency and highest data integrity choices available for each element.

Software development lifecycle

The application is developed in a Development environment, then deployed to a Preproduction server for testing and finally, upon approval, deployed to the production server. This is managed fully through Microsoft Azure DevOps, with automated pipelines ensuring only vetted artefacts reach each stage, and ensuring a number of approvers have actively engaged with the pushed update before it goes live.

Certification Held

Microsoft Azure maintains certification with robust security standards, such as ISO 27001, SOC 1/2/3 and PCI DSS Level 1. We operate a shared responsibility model in the Cloud, under which Microsoft is responsible for the security of the underlying Cloud infrastructure (Security of the Cloud) and Kinseed is responsible for the security of the MediWork data and applications (Security in the Cloud). Microsoft has teams of Solutions Architects, Account Managers, Consultants, Trainers and other staff in the UK trained on cloud security and compliance to assist Microsoft customers in achieving high levels of security and compliance in the Cloud, following Cloud Security Best Practices.

Kinseed Limited is also fully certified and compliance in line with the following governing standards,

- ISO 9001, ISO 27001
- Cyber Essential and Cyber Essential Plus
- ICO Certified
- NHS Digital – Data Security and Protection Toolkit Kinseed (YGM1H) - Exceed Standards

Location of Servers

The live system is located in UK. For security purposes, Microsoft does not reveal the precise location of these Datacentres.

Pre and Post Engagement

We offer comprehensive onboarding and offboarding support, ensuring a smooth transition for your team. As part of the onboarding process our approach considers an enterprise level architecture view - people, processes and technology, together with an agile methodology for early identification and management of risks / issues, through change management. We mobilise the right resources appropriately to work in partnership with the customer. We will work with the client to agree a governance model as part of the enegement process covering a complete customer lifecyle framework. All our products and services are implemented on a robust Microsoft stack based on the Azure cloud platform (availability SLA 99.9%). We build with Continuity, Security and Safety in mind from the ground-up, and this is reflected in the way we architect and govern our solutions. As a Microsoft Cloud Partner, we use Microsoft 365 in the workplace, and related DevOps, Configuration Management, Cyber Security, GDPR Data Protection and Privacy tools and technologies on the periphery. Our general internal governance controls and the ISO-9001 and ISO-27001 policies we adhere to ensure we are always compliant with governance and regulatory needs.

Kinseed will customise training based on your specific needs. Training modules will be tailored to specific roles and will cover all aspects of both operation and configuration of the system. We will run as many training sessions necessary (based on the agreed prpject scope) to ensure every team member is happy and confident with using the application. We will produce any required materials, short videos, guidelines etc.

As mentioned above, MediWork is powered by Microsoft Azure and is backed with Microsoft's service availability levels of 99.5%. Kinseed will respond to all incidents and work in accordance with the agreed Service Levels to rectify them. The following is a guideline to enable the appointment of an appropriate prioritisation which is set by mutual agreement between the customer and Kinseed. Priorities are to be distinguished by the effect on internal and external customers.

Severity	Maximum time required to resolve	Examples
1 - Critical	4 hours	System completely unavailable
2 - High	12 hours	Key components of the system are unavailable
3 - Medium	24 hours	Non-critical components of the system are unavailable
4 - Low	48 hours	The system is operating but through the use of non-standard workarounds