2025/09/10

Access Care Planning

FACT SHEET

Contents

Introduction

This Fact sheet provides the detail required for Data Privacy Impact Assessments, processing information that supports our terms and conditions and general security relating to the product and associated services.
Further information can be found on our Customer Security Portal
This product is available in the following regions: UK

Subject Matter

- Privacy Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.
- It fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

The Product	
Name of Product / System	Access Care Planning
Set up options	Saas
Purpose of the Software	To record service user and patient information. This includes (but is not limited to) patient's medication condition, care plans, medical assessments, reviews etc.
Product Category	Health & Social Care - HSC
The Data	
Duration of Processing	Processing will continue for the duration of the active contract. Access does not apply retention schedules to client data other than for backups (see backup section) and deletion of data on termination of contract in line with our Exit policy (unless there is a legal requirement for Access to retain the data)
Nature of Processing	Hosted/ SaaS - We receive data uploaded to the service by users, which is stored in a cloud environment in accordance with the options selected by You. Users may instruct the service to share some or all of the data with other users or groups/classes of users.
Purpose of Processing	The data is entered or imported into Access Care Planning via Access People Planner, or by the client The type of data captured, held, and processed is configured by our clients / based on their needs *Further details about Access People Planner can be found in Access People Planner Product Fact Sheet*
Categories of Data Subject	Data may be related to the following categories of Data Subjects:

	Medical/ Patients /Applicants /Employees /Customers /Prospects /Service Users/ Carers.
Personal information, that on its own or with any other data in the system, can identify an individual	Type of data depends on the way our customers configure the system. Examples of PII First Name / Surname Email Title DOB Gender Address Secondary Telephone Photo Key Safe Numbers (Clients Only) + anything else configured by the client
Special categories of Data stored ○ Race / Ethnic origin ○ Political opinions /Religion / Philosophical beliefs ○ Trade union membership ○ Genetic data /Biometric data / Health ○ Sexual Orientation / Concerning a natural person's sex life	Health history - Treatments and care plans - Daily activities + anything else configured by the client (eg. custom case fields, activities, form definitions)
The Rights of the Individual	
Subject Access Requests	Access Care Planning includes functionality to provide full access to individuals to their data, using built-in role based access control features. Furthermore it provide APIs to extract the data and clients can store it any format in their systems. This would require assistance from the Access Care Planning development team.
Portability information	This would require assistance from the Access Care Planning development team. The product API can supply almost all data in JSON, other data can be queried by the developers from the DB and exported as CSV, .bak, or PDF.
Data Amendments	Yes. Data is typically stored as forms and case fields. Clients can change these whenever they wish, only IDs/primary identifiers and timestamps cannot be altered.
Details of Automated decision-making processes	Access Care Planning configuration includes workflow logic. Clients can add workflow logic to their solution and can amend or suspend these workflow rules any time as required. “Out of the box”, it does not have any automated decision making processes
Right to Erasure (Right to be Forgotten)	Information can be manually deleted or can be anonymised with the assistance of Support / Development
Bulk data archiving/ deletion capability within this product	Not within the product, this would be achieved via the development team running DB scripts to delete (and possibly archive depending on the exact data in question).

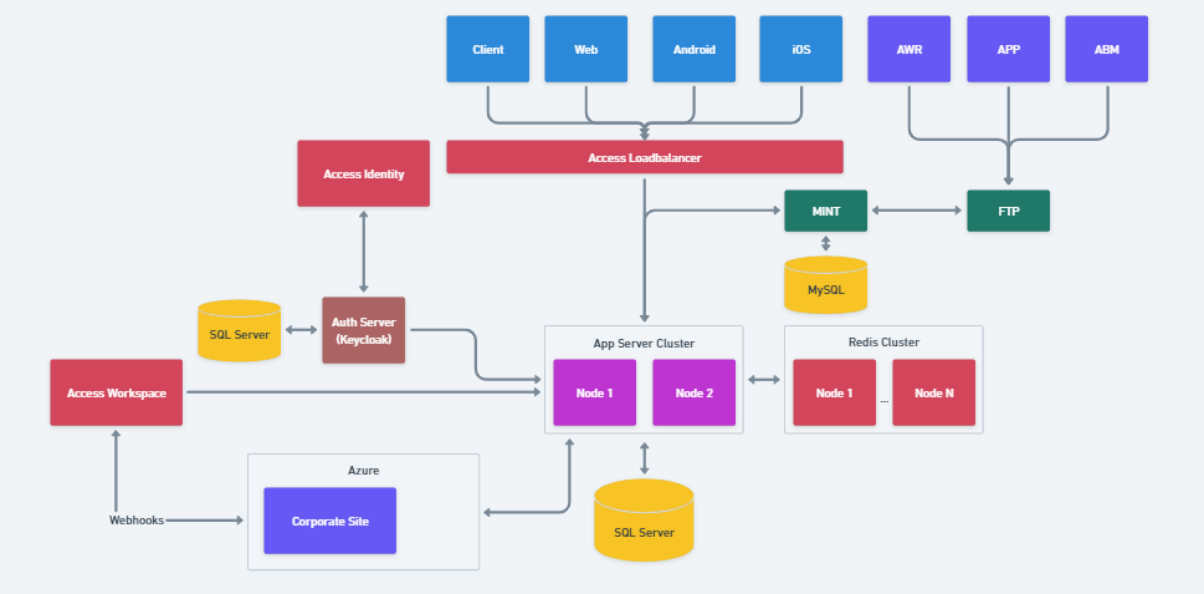
Retention schedules can be set within the product	No
Anonymisation capability	Yes – Manual process (database script by the development team). Name, address, telephone numbers, email can be anonymised.
Pseudonymisation capability	No
Access Control & Auditing	
Is this product available in Evo Platform	Yes
Who - apart from the customer has ongoing access to client data and for what purpose	Development, Support, On-boarding teams as required by client (initial settup, support, development)
Geographical Location of those teams	UK & Romania
How do that technical team access the software for support and operational purposes	Via UI using client user/admin impersonation or support user login.
Who has access to the hosted database (not the software) and for what purposes	IT&O, Development, HSC Technical Support as required by client for Operational and Technical support
Geographical Location of those teams	UK & Romania
How do that team access the database for support and operational purposes	MySQL Workbench or MSSQL Management Studio on internal network.
How is access control to the product managed for customer users – what protocols does it support?	Individual login via username and password via direct to URL access. Access Evo for Care SSO. Access Identity can also be used Access Evo Core Product Fact Sheet and Access Identity Product Fact Sheet should be consulted for further details
Does the product support role-based profiles / who determines them and who administers	Access control is controlled using Access Care Planning "roles-based" access control engine. Tenant administrators can configure roles and assign specific permissions to these roles.
Password Policy	Must be at least 8 characters long Must contain at least 6 alphabetic characters Must contain at least 1 numeric character Must contain at least 1 special character In Access Identity, the password policy is set by client
Password Security information	Encrypted HASH key of password is stored in the Database
Password Expiry	None In Access Identity, the expiry policy is set by client

Number of log-in attempts before account is locked	10 failed attempts will lock login for the account for 12 hours. In Access Identity – set by client
Successful and Failed login attempts recorded?	Yes
Other areas of the software where actions are recorded and auditable	Login Any changes to patient records
Storage of Audit Logs	Logs for API interactions are kept for two weeks. Logs for updating a person's record are kept in the DB indefinitely.
Is there an automatic time out after inactivity - please state what time	Yes, 60 minutes (default). Can be configured by the client.
Does this product redirect a user to a card payment provider	NO
Outputs to other systems / externally or internally	Outputs to Extraction Engine and Access People Planner
Is Wootric Feedback enabled for this Product?	Yes
Product Security	
APIs in use	Yes, Spring Boot & Spring Security handle HTTPS calls
Are there any third-party components in the software? If yes, how do we ensure there are no vulnerabilities after use and in the future?	Hibernate, Spring, Freemarker, and React. Development team to monitor updates and deploy as required.
Data Encryption in Transit	Yes – TLS V1.2 and Secure File Transfer Protocol encryption
Keys Managed by	Development
Data Encryption at rest	Yes - Bitlocker encryption & AES 256-bit encrypted backups
Email functionality	Yes
Email provider	smtp.accessacloud.com
Geographical routing of email	UK
Data Storage formats	Relational Database Records – MSSQL
Cookie information	Session cookies for user authentication and applications settings and preferences, tracking cookies (Google Analytics)
Physical & Network Security/Storage	
Location of server / physical storage / file system/ Data Centre Provider / Geographical location	Telehouse Data Centre London & Woking

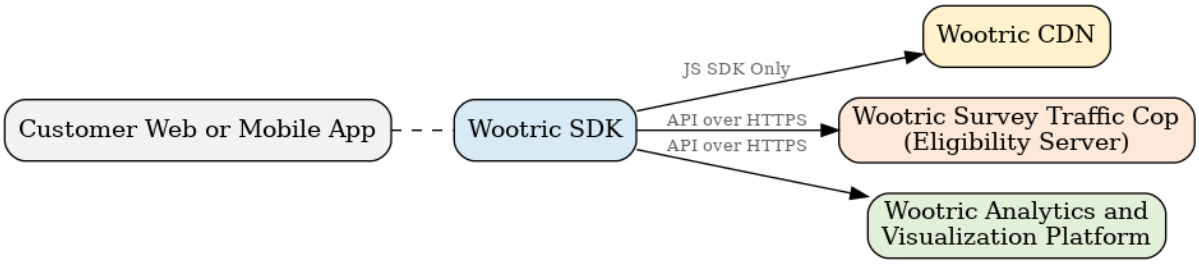
Who manages the environment	Access Cloud Hosting Services
Firewall Information	Includes but not limited to Palo Alto and Cisco Firepower modules Server Firewalls - Windows Firewall Distributed Firewalls – VMWare NSX
Intrusion Detection	Access uses a combination of technologies Layer 7 Firewalls IDS/IPS/Malware/Threat protection Behavioural Analytics & Heuristics endpoint protection Phishing Protection Network Segregation MFA Conditional Access Controls
Antivirus in use on Servers	Cortex XDR
Other security features	Multiple – available in the Hosting Security Overview document on the Security Portal
Is this a multi-tenanted database?	Yes
How the client is data segregated from other Clients in the hosted / Cloud environment	Separated at Database Level by Tenant (customer) ID
Other set up options available (i.e. isolated/shared)	Shared by default. Dedicated servers and DBs can be set up of required as an additional service.
Backup details / Storage/ Encryption and Retention	SQL Transaction log back up every 15 minutes, kept for 28 days Daily (10 pm) backup, kept for 28 days Weekly (Saturday) backup, kept for 3 Months Backups are stored within a multi tenancy data vault and are encrypted at rest Equinix LD3 - Slough
Backups managed by	Access IT&O
Business Continuity and Disaster Recovery details	Rebuild VM with VMware last snapshot (MSSQL), restore DB using previous backup + logs files (MSSQL)
What is the recovery time objective (RTO) and recovery point objective (RPO) for restore	RTO 12h RPO 15 min
Segregation of Production and Development environments.	Logically and Physically
If there is a web service Is there a mechanism that restricts access to the Web Service	Yes, restricted URIs which require an authenticated user.
About the Mobile App	
Is there a mobile app	Yes

What functionality does it provide	Care administration flow
How is data secured between the app & the server?	HTTPS (SSL)
Is Data stored on the device? (If yes, what data? for how long?)	Yes - service user details, rota, forms/assessments for up to 45 days (user configurable)
Format of stored data	Encrypted SQLite database, Keychain secure storage, User Defaults text file for non-sensitive information
Access Co-Pilot	
Purpose of the connection with Co-Pilot	Available via Access Evo Core. Enabling customers to use AI with application data.
Description of the Personal Data that may be processed by Access Co-Pilot	First name Surname Address Phone number NI Number (Applicant/Employee). Next of Kin Emergency Contact Details (Name & Address) Gender Email Address Other fields configurable by the client Access to this data, via Copilot, is controlled by the user permissions and level of access
Additional information about Access Co-Pilot can be found on the Access Evo Product Fact Sheet	
Exit Arrangements	
How is data returned to clients on termination Access Provides / Self-Serve / Bit of both	Access Provides
What is the standard format	.pdf or .csv files provided via sFTP / .bak files – DB exports provided via sFTP.
How is the data deleted or anonymised	Anonymised via a DB script or through People Planner integration
How is that achieved?	Via a script

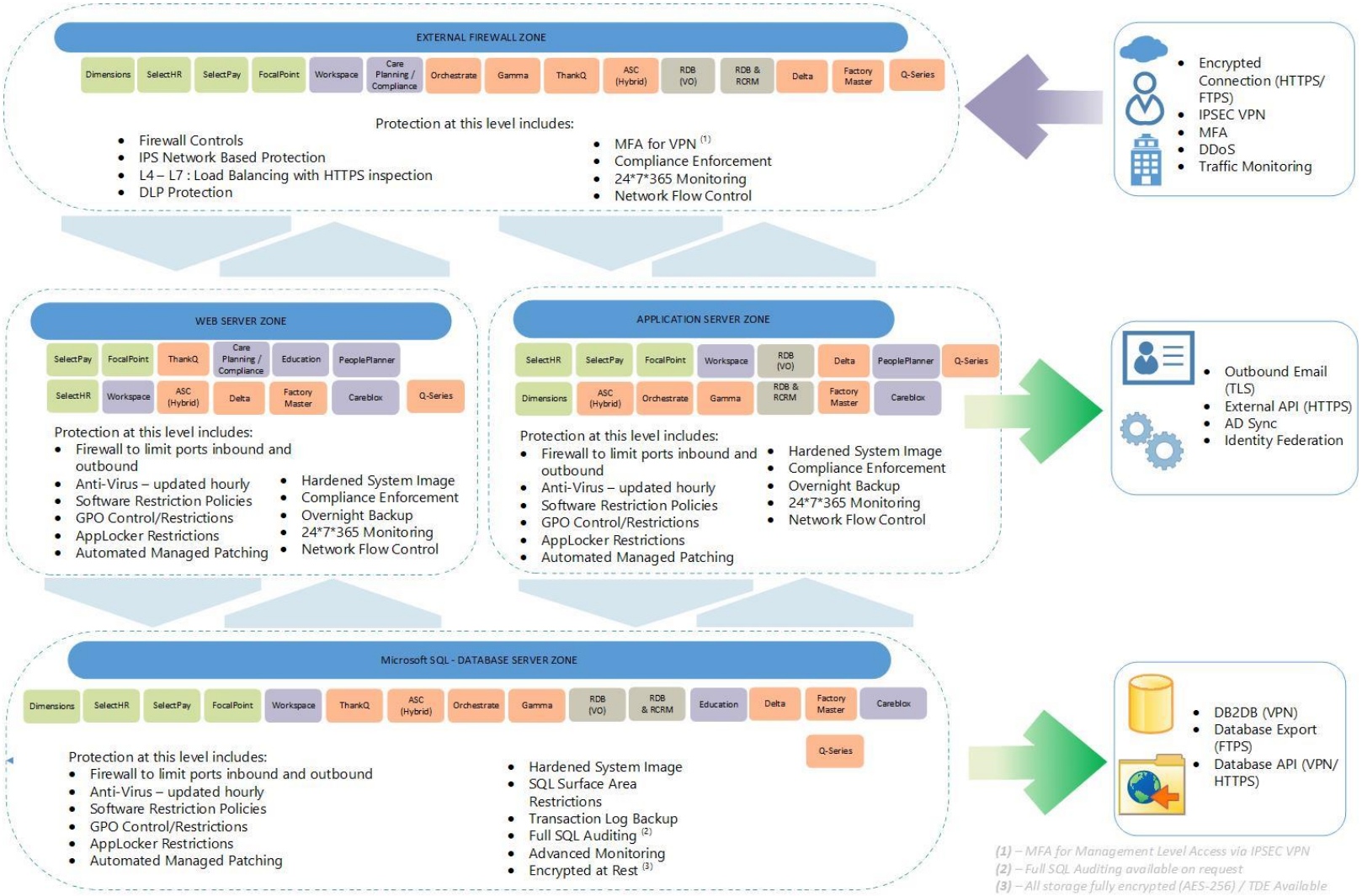
Product Data Flow



Wootric Data Flow



Network Diagram



Schedule 1 – Sub-Processors

Sub-processor Name	Category	Sub-processor Main Location(s)	Nature of the Processing	Location of the Processing	Is the data stored in the location of Processing	Safeguards / Legal Data Privacy Frameworks
Access Workspace Romania	Affiliate	Romania	Onboarding, professional services, support, technical support, offboarding	EU	No	Intra-Group Data Processing Agreement
Access GOC Malaysia Sdn Bhd	Affiliate	Malaysia	Onboarding, professional services, support, technical support, offboarding	Malaysia	No	Intra-Group Data Processing Agreement
Access UK LTD	Affiliate	United Kingdom	Onboarding, professional services, support, technical support, offboarding	United Kingdom	Yes	Intra-Group Data Processing Agreement
Microsoft 365	Processor	United Kingdom	document creation and storage	United Kingdom	Yes	EU SCCs and UK IDTA

Schedule 2 – Processing Activities		
This list is non-exhaustive but is intended to describe some of the key processing activities involved in providing the Access Product described in this product fact sheet to you. For processing activities, we carry out as an independent controller, please see our Privacy Notice.		
	Processor	**Controller**
Onboarding	Activities may include data collection, data manipulation and or upload.	Information pertinent to key persons may be collected and processed by us. For example, a key person for implementation, administrative and/or for financial matters (e.g., payment of invoices).
		All login information to access the product.
BAU	Activities may include hosting and/or extracting of your data and transferring your data (all or part, as required) to the necessary third parties. Including doing anything with your data which is otherwise necessary to fulfil any professional service requests from you.	Telemetry data and other general product usage data.
		Feedback about the product from end users.
		Processing any of your data to ensure the security, integrity, availability, and resilience of the Access Product(s). This includes activities such as threat detection and response, system monitoring, infrastructure maintenance, server patching, and backup and restore procedures.
		Processing of any data collected through cookies (or similar technologies) that we might place on the end user's device.
Support	Activities may include analysing, searching through, or otherwise manipulating and or deleting your data (or part thereof), as per your instruction or as needed to resolve an issue.	Data collected by us using our support platforms, online forms, telephone calls to us etc., pertinent to you raising a support case with us.
Offboarding	Activities may include returning your data or making your data available for download on a self-serve basis and deleting your data.	Information of the person determining the instructions at cessation of the relevant contract.

Schedule 3 – AI Processing					
AI Purpose	**Data Types**	**AI Vendor**	**Processing Location**	**Retention**	**Automated Decisions**
[Specific business function the AI performs, e.g., "validation of data or change formatting type of data"]	[Exact personal data categories sent to AI, e.g., "email addresses, message content, user names"]	[AI service provider name and model, e.g., "OpenAI GPT-4" or "Self-hosted"]	[Country/region where AI processing occurs]	[How long data stays in AI system, e.g., "24 hours" or "immediately deleted"]	[Yes/No - if yes, describe what decisions AI makes automatically]