fava

Service Definition

Fava Genomics Results Portal

1. Service overview

The Fava Genomics Results Portal is a cloud-based software service designed to enable individuals to securely access, understand, and engage with their genomic results. The service presents genomic information in a clear, accessible, and patient-friendly way, supporting informed health and lifestyle decisions.

The portal is intended for use within healthcare and public-sector health programmes, including research studies and population genomics initiatives. It can be launched as a standalone web application or accessed in context from existing patient portals or digital health applications, depending on local implementation requirements.

2. Service scope and functionality

The service provides a secure, web-based interface for viewing genomic results and related explanatory content. Core functionality includes secure access to individual results, clear presentation of genomic insights, and supporting information to aid understanding.

The portal is designed to operate as part of a broader digital health ecosystem and can integrate with upstream systems via APIs to receive results data and enable contextual access. The service is delivered as a managed SaaS offering, with Fava responsible for platform operation, maintenance, and ongoing improvement.

3. Getting started and onboarding

Fava supports buyers through a structured onboarding approach appropriate to the deployment context. This typically includes configuration of the portal to align with programme scope, governance requirements, and branding where appropriate.

End users do not require formal training to use the service. The portal is designed to be intuitive and self-guided, supported by clear in-service explanations and accessible user guidance. Documentation for buyers and implementation teams is provided in accessible formats, including HTML and PDF.

4. Service constraints

The service is accessed via a modern web browser and does not require local software installation. Internet access is required. Planned maintenance is scheduled where possible outside of normal working hours and communicated in advance. Emergency maintenance may be required to address security or stability issues.

Where the portal relies on upstream systems for data provision or contextual launch, availability of those systems may affect end-to-end user experience.

5. Availability and service levels

The service is designed for high availability and is hosted on resilient cloud infrastructure. Fava targets a monthly service availability of 99.5%, excluding planned maintenance.

Service levels, including availability commitments and support arrangements, are agreed as part of each Call-Off Contract. Where service

levels are not met, service credits may be applied in line with agreed contractual terms and typically offset against future charges.

6. Resilience and business continuity

The service is built using a cloud-native architecture designed to reduce single points of failure and support scalability. Core components are deployed with redundancy, and monitoring is used to identify and respond to service issues.

Datacentre resilience, including physical security, power, cooling, and environmental controls, is provided by the underlying cloud infrastructure provider, who operates accredited facilities. Further details on resilience arrangements can be provided on request.

7. Security governance

Security governance is embedded into the design, development, and operation of the service. Responsibility for security sits with senior leadership, with oversight of risk management, secure development practices, and incident response.

The service follows cloud security best practices and is supported by external penetration testing and vulnerability management. Fava is formalising its governance arrangements through implementation of a quality management system (QMS) and alignment with NHS Digital Technology Assessment Criteria (DTAC).

8. Secure development and change management

The service is developed following defined internal processes for secure software development. Changes to application code and configuration are

controlled, reviewed, and tracked using version control and change records.

Proposed changes are assessed for potential impact on security, performance, and service reliability. Changes are tested prior to release and deployed in a controlled manner. These processes are being formalised as part of the QMS to support consistent governance and continuous improvement.

9. Vulnerability management and protective monitoring

Vulnerabilities are identified through a combination of external penetration testing, routine security review, and monitoring of relevant threat intelligence. Risks are assessed based on severity and impact, prioritised, and tracked to remediation.

Protective monitoring is used to identify potential security or service issues through logging, monitoring, and alerting of key events. Potential compromises are investigated promptly, with incidents escalated and managed through defined response processes.

10. Incident management

The service follows defined incident management processes to identify, assess, and respond to incidents. Pre-defined processes are in place for common event types, including service disruption and security incidents.

Users and buyers can report incidents through agreed support channels. Incidents are logged, investigated, and prioritised based on impact and severity. Where appropriate, incident updates and summary reports are provided to buyers.

11. Identity, access control, and audit

End users authenticate using secure, passwordless authentication via time-limited email login links. This approach avoids the need for passwords while maintaining controlled access to individual results.

Access to management interfaces and support channels is restricted to authorised staff using role-based access controls and multi-factor authentication. Audit logs are maintained for user and supplier actions and retained for at least 12 months. Audit information is made available to buyers on request.

12. Data storage and protection

Data is stored and processed in the United Kingdom using public cloud infrastructure. Data is encrypted in transit using TLS 1.2 or above and encrypted at rest using cloud-provider-managed encryption.

Physical datacentre security and equipment disposal are managed by the cloud infrastructure provider. Data sanitisation is performed using cryptographic erasure and logical deletion processes when data is no longer required or at contract end.

13. Data export, retention, and exit

Users can download or print their genomic results in accessible formats such as PDF. Buyers may also request structured export of programme data where appropriate.

At the end of the contract, access to the service is terminated, data is securely exported where required, and remaining data is securely deleted in line with agreed retention policies. Standard exit support is included, with additional bespoke support available by agreement.

14. Support model

Support is provided via email or ticket-based channels during agreed support hours. Outages and significant service issues are communicated directly to nominated buyer contacts.

Support levels and response times are defined as part of each Call-Off Contract. The service does not include a named technical account manager as standard, though additional support arrangements can be agreed where required.

15. Pricing, trials, and discounts

Pricing is agreed per Call-Off Contract based on scope and usage. Special pricing may be available for educational and research organisations by agreement.

Free or trial access may be offered on a time-limited basis for evaluation, research, or pilot purposes. Trials include agreed functionality within a defined scope but exclude production deployment and full support.