fava

Service Definition

Fava Clinical Genomics Platform

1. Service overview

The Fava Clinical Genomics Platform is a cloud-based software service designed to support the safe and effective use of genomic data within everyday clinical workflows. The service enables genomic insights to be translated into actionable clinical decision support, supporting clinicians in real-world care settings.

The platform is designed to integrate with existing clinical IT systems, allowing genomic insights to be accessed in context without requiring clinicians to manage separate logins or workflows. The service is intended for use across healthcare, research, and public-sector health environments and is configurable to local clinical pathways, governance requirements, and service models.

---

2. Service scope and functionality

The service provides a configurable platform for managing, interpreting, and presenting genomic insights in clinical contexts. Core functionality includes secure data handling, configurable decision support logic, and role-appropriate presentation of information to end users.

The platform supports integration with external systems via APIs and standards-based approaches, enabling deployment within existing digital health ecosystems. 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 an implementation and onboarding process tailored to the scope and context of deployment. This typically includes collaborative configuration of the service to reflect local clinical workflows, pathways, and governance requirements.

Training and enablement may be provided for implementation teams and administrative users. End users, such as clinicians, are supported through role-appropriate guidance, documentation, and in-context use within existing systems. User documentation is provided in accessible formats, including HTML and PDF.

---

4. Service constraints

The service is accessed via web browsers and APIs and does not require local software installation. 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.

The service relies on integration with upstream clinical systems for certain functionality, and availability of those systems may affect end-to-end workflows.

---

5. Availability and service levels

The service is designed for high availability and is hosted on resilient public 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 platform 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 to buyers 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 the implementation of a quality management system (QMS), aligned with ISO 9001 principles, and is working towards Cyber Essentials Plus and NHS Digital Technology Assessment Criteria (DTAC) alignment.

---

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 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 via their primary clinical system. When the service is launched in context, user identity and role are asserted by the upstream system and trusted by the service, avoiding the need for separate credentials.

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 via the support team.

---

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

Buyers can request export of their data in open formats, such as CSV or structured formats, at contract end. Data export is supported as part of the offboarding process.

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 in the contract price, 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 currently include a named technical account manager as standard, but 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.