INFORMED GENOMICS LTD. (IGL) TRADING AS

NONACUS CLINICAL SERVICES (NCS)

API TERMS OF USE

(VERSION 2.0 - LAST UPDATED 16 MAY 2025)

You (the 'Customer') has requested and NCS has agreed to provide whole genomic testing services, as set out in the Quotation, Service Level Agreement and Business Terms and Conditions (together referred to as 'Main Agreement'). Pursuant to the Main Agreement and technical on-boarding assessment, you (the 'Customer') have requested and NCS has agreed to provide you with a clinical report via NCS's API.

By accessing or using NCS's API, you are agreeing to be bound by these API Terms of Use ('API Terms') and to comply with any accompanying documentation (API Documentation) that applies to your use of NCS's API. You represent and warrant that you ('the Customer') have the authority to accept these API Terms on behalf of yourself, a company, and/or other entity, as applicable. We may change, amend or terminate these API Terms at any time. Your use of NCS's API after any change or amendment means you agree to the new API Terms. If you do not agree to the new API Terms or if we terminate these API Terms, you must stop using NCS's APIs.

Agreed terms

1. Interpretation

1.1 The definitions and rules of interpretation in this clause apply in this licence.

API: NCS's hCRM application programming interface (API) made available to Customer by NCS including, without limitation, through the azurewebsites.net domain each as updated for the Customer from time to time.

API Call: each call from a Customer Application via the API to interact with the NCS's hCRM.

API Documentation: means the API documentation made available to Customer by NCS which forms Annex A.

API Key: the security key NCS makes available for Customer to access the API.

API Terms: the terms of this agreement.

Customer: means the person or entity who has agreed to these API Terms of Use (‘API Terms’).

Customer Application: any Customer Applications developed by, or on behalf of, or used by the Customer to interact with the API and NCS’s hCRM.

Authorised Users: the users authorised by the Customer to access the API on behalf of the Customer via the API Key.

Customer System: the Customer Application, together with any other network and information systems (including any hardware, software and other infrastructure) and processes operated by or on behalf of the Customer that is used to access the API, make an API Call or otherwise communicate or interact with ncs’s hCRM.

Data Protection Laws: means, as applicable: a) the General Data Protection Regulation ((EU) 2016/679) (‘EU GDPR’); b) the Data Protection Act 2018; c) the retained EU law version of GDPR (“UK GDPR”) by virtue of section 3 of the European Union (Withdrawal) Act 2018 (EU GDPR and UK GDPR together referred to as ‘GDPR’); d) any laws that replace, extend, re-enact, consolidate or amend any of the aforementioned legislation or regulation; and any Local Privacy Laws.

End Users: any individuals (such as the Customer's employees, contractors, or agents) whom the Customer permits or enables to use or access the API.

Effective Date: the date the parties have entered into the API Terms.

hCRM: NCS's healthcare customer relationship management system (hCRM).

NCS: means Informed Genomics Limited, trading as Nonacus Clinical Services, a company incorporated in England and Wales with registered number 13082290 whose registered address is at Unit 5, Quinton Business Park, 11 Ridgeway, Quinton, Birmingham, B32 1AF.

Intellectual Property Rights: patents, utility models, rights to inventions, copyright and related rights, trade marks and service marks, trade names and domain names, rights in get-up, goodwill and the right to sue for passing off or unfair competition, rights in designs, rights in computer software, database rights, rights to preserve the confidentiality of information (including know-how and trade secrets) and any other intellectual property rights, including all Customer Applications for (and rights to apply for and be granted), renewals or extensions of, and rights to claim priority from, such rights and all similar or equivalent rights or forms of protection which subsist or will subsist, now or in the future, in any part of the world.

Local Privacy Laws: means the national or federal laws that apply to a specific geographical area which govern how personal information (including 'Customer Personal Data' and 'Customer Patient Data') is to be protected and may be shared and processed by NCS.

Main Agreement: means the combination of the: (a) Quotation; and (b) Service Level Agreement, incorporating the Business Terms and Conditions (as published on the NCS website).

Services: means the service provided by NCS to the Customer as agreed in the Quotation and associated Service Level Agreement and incorporating the Business Terms and Conditions (together referred to as 'Main Agreement').

Virus: any thing or device (including any software, code, file or program) which may: prevent, impair or otherwise adversely affect the operation of any computer software, hardware or network, any telecommunications service, equipment or network or any other service or device; prevent, impair or otherwise adversely affect access to or the operation of any program or data, including the reliability of any program or data (whether by re-arranging, altering or erasing the program or data in whole or part or otherwise); or adversely affect the user experience, including worms, trojan horses, viruses and other similar things or devices.

Vulnerability: a weakness in the computational logic (for example, code) found in software and hardware components that when exploited, results in a negative impact to the confidentiality, integrity, or availability, and the term **Vulnerabilities** shall be construed accordingly.

1.2 Clause, Schedule and paragraph headings shall not affect the interpretation of API Terms.

1.3 Unless expressly stated otherwise, or the context otherwise requires:

(a) words in the singular shall include the plural and in the plural shall include the singular;

(b) A reference to a statute or statutory provision is a reference to it as amended, extended or re-enacted from time to time;

(c) a reference to one gender shall include a reference to the other genders; and

(d) any words following the terms **including, include, in particular, for example** or any similar expression shall be interpreted as illustrative and shall not limit the sense of the words, description, definition, phrase or term preceding those terms.

1.4 In the case of conflict or ambiguity between any provision contained in the body of API Terms and any provision contained in the Annex(es), the provision in the body of API Terms shall take precedence.

1.5 A **person** includes a natural person, corporate or unincorporated body (whether or not having separate legal personality) and that person's personal representatives, successors and permitted assigns.

1.6 The Annex(es) form part of API Terms and shall have effect as if set out in full in the body of API Terms. Any reference to API Terms includes the Annex(es).

2. Licence

2.1 In consideration of the Fee paid by the Customer to NCS for the provision of Services under the Main Agreement, NCS grants to the Customer a non-exclusive licence during the term of the Main Agreement for the Authorised Users to access the API solely for the purposes of:

(i) internally developing the Customer Applications that will communicate and interoperate with NCS's hCRM; and

(ii) making API Calls in order to connect to NCS’s hCRM.

2.2 The Customer's sole means of accessing the API for the purposes of clause 2.1 shall be via the API Key.

2.3 In relation to the scope of use set out in clause 2.1,

(a) the Customer shall not (and shall procure End Users do not):

i. remove any proprietary notices from the API;

ii. use the API in any manner or for any purpose that infringes, misappropriates, or otherwise infringes any Intellectual Property Right or other right of any person, or that violates any applicable law;

iii. design or permit the Customer Applications to disable, override, or otherwise interfere with any NCS-implemented communications to end users, consent screens, user settings, alerts, warning, or the like;

iv. use the API, including in any of the Customer Applications, to replicate or attempt to replace the user experience of NCS’s hCRM;

v. attempt to cloak or conceal the Customer's identity or the identity of the Customer Applications when requesting authorisation to use the API or making an API Call;

(b) The Customer shall (and shall procure End Users) agree and adhere to the API Key Security & Usage Compliance Form contained in **Annex A**.

2.4 Except as expressly stated in this clause 2, the Customer has no right (and shall not permit any third party) to copy, adapt, reverse engineer, decompile, disassemble, modify, adapt or make error corrections to the API or NCS’s hCRM, in whole or in part (except to the extent that applicable law overrides this provision or any part hereof).

2.5 The Customer shall not use the API other than as specified in this clause 2 without the prior written consent of NCS.

2.6 Without prejudice to its other rights and remedies under API Terms, should the Customer use the API other than as specified in this clause 2 without the prior written consent of NCS, NCS may, in its sole discretion terminate API Terms, or suspend the Customer's access and use to the API, on written notice with immediate effect.

2.7 NCS shall be entitled to suspend the Customer's access to, and use of, the API under clause 2.6 until such time as the breach is remedied to NCS's reasonable satisfaction.

3. Customer responsibilities

3.1 The Customer must obtain an API Key through the registration process available at azure.websites.net domain to use and access the API. The Customer may not share the API Key with any third party other than Authorised Users, must keep the API Key and all log-in information secure, and must use the API Key as the Customer's sole means of accessing the API. The API Key may be replaced at any time by NCS on notice to the Customer.

3.2 The Customer shall:

(a) ensure that no End User other than an Authorised User accesses the API.

(b) without affecting its other obligations under API Terms, comply with all applicable laws and regulations with respect to its activities under these API Terms;

(c) carry out all of its responsibilities set out in these API Terms in a timely and efficient manner. In the event of any delays in the Customer's provision of such assistance as agreed by the parties, NCS may adjust any agreed timetable or delivery schedule as reasonably necessary;

(d) keep a complete and accurate record of:

(i) its End Users;

(ii) its development of the Customer Application;

(iii) its use of the API;

(iv) its other obligations under API Terms,

and produce such records to NCS on request from time to time; and

(e) notify NCS as soon as it becomes aware of any unauthorised use of the API by any person.

3.3 Subject to clause 10, the Customer is responsible and liable for all uses of the API resulting from access provided by the Customer, directly or indirectly, whether such access or use is permitted by or in breach of API Terms, including use with any Customer Application or third-party software. Without limiting the generality of the foregoing, the Customer is responsible for all acts and omissions of End Users in connection with the Customer Application and their use of the API, if any. Any act or omission by an End User that would constitute a breach of API Terms if taken by the Customer will be deemed a breach of API Terms by the Customer. The Customer shall take reasonable efforts to make all End Users aware of these API Terms, in particular those contained in Annex A, as applicable to such End Users and shall cause End Users to comply with such provisions.

3.4 The Customer shall monitor the use of the API for any activity that breaches applicable laws, rules, and regulations or any terms and conditions of API Terms, including any fraudulent, inappropriate, or potentially harmful behaviour, and promptly restrict any offending users of the Customer Applications from further use of the Customer Applications.

4. Maintenance releases

4.1 NCS shall make Maintenance Releases available to the Customer no later than such releases are generally made available to its other customers.

4.2 The Customer is required to make any change to the Customer Application that is required for integration as a result of such Maintenance Release at the Customer's sole cost and expense as soon as reasonably practicable after receipt.

5. Audit

5.1 NCS, or its representative, may monitor and audit the Customer's use of the API to ensure the Customer is complying with the terms of API Terms, provided any physical audit shall take place on reasonable advance notice and at reasonable times. Such audit may include an audit of the Usage Data to verify the name and password of each End User.

5.2 If the audit referred to in clause 5.1 reveals that the API has been used or accessed other than in accordance with API Terms, then, without prejudice to the NCS's other rights, the Customer shall promptly disable such access and use and the NCS shall be entitled to revoke any existing passwords, or not issue any new passwords, to any End User so implicated in the unauthorised use or access.

6. Confidentiality and publicity

6.1 Each party shall, during the term of API Terms and thereafter, keep confidential all, and shall not use for its own purposes (other than implementation of API Terms) nor without the prior written consent of the other disclose to any third party (except its professional advisers or as may be required by any law or any legal or regulatory authority) any information of a confidential nature (including trade secrets and information of commercial value) which may become known to such party from the other party and which relates to the other party or any of its Affiliates, unless that information is public knowledge or already known to such party at the time of disclosure, or subsequently becomes public knowledge other than by breach of this licence, or subsequently comes lawfully into the possession of such party from a third party.

6.2 For the avoidance of doubt the API and the API Key shall be considered the confidential information of NCS for the purposes of these API Terms.

6.3 NCS shall be entitled to reference the Customer as a user of the API in NCS's general marketing literature, including NCS's website and other online platforms. The reference to the Customer for these purposes may include a reference to the Customer's corporate name and to any of its trade names and trade marks.

6.4 Save as provided for in clause 6.3, no party shall make, or permit any person to make, any public announcement concerning API Terms without the prior written consent of the other parties (such consent not to be unreasonably withheld or delayed), except as required by law, any governmental or regulatory authority (including, without limitation, any relevant securities exchange), any court or other authority of competent jurisdiction.

7. Data protection

7.1 Both parties will comply with all applicable requirements of the Data Protection Laws. This clause 7 is in addition to, and does not relieve, remove or replace, a party's obligations or rights under the Data Protection Laws.

7.2 NCS may collect certain information about the Customer and its personnel, representatives and agents, including End Users, in connection with API Terms, as set out in the then-current version of the NCS's privacy policy, available at https://nonacus.com/services-privacy-notice/ (**Usage Data**). This may include information collected through the API or NCS’s hCRM. By entering into API Terms, and accessing, using, and providing information to or through the API or NCS’s hCRM, Customer consents, and shall procure all required consents from its personnel, representatives and agents (including End Users) to all actions taken by the NCS with respect to the Usage Data in compliance with the then-current version of the NCS's privacy policy, available on the NCS website. In the event of any inconsistency or conflict between the terms of the then-current privacy policy and API Terms, the privacy policy will take precedence.

7.3 The parties acknowledge that the Usage Data is processed by NCS as a controller for the purposes of the Data Protection Laws.

7.4 Without prejudice to the generality of clause 7.1, the Customer will ensure that it has all necessary appropriate consents and notices in place to enable lawful transfer of any personal data (including Usage Data) to NCS for the duration and purposes of these API Terms so that the NCS may lawfully use, process and transfer this data in accordance with these API Terms; including in relation to the role outlined in clause 7.3.

8. Systems and security

8.1 The Customer:

(a) is responsible for the operation and security of the Customer System and the Customer Application;

(b) shall ensure that the Customer System and the Customer Application comply with any relevant specifications provided by the NCS from time to time;

(c) shall be, to the extent permitted by law and except as otherwise expressly provided in these API Terms, solely responsible for procuring, maintaining and securing its network connections and telecommunications links from the Customer System and the Customer Application to NCS's hCRM, and all problems, conditions, delays, delivery failures and all other loss or damage arising from or relating to the Customer's network connections or telecommunications links or caused by the internet; and

(d) will take reasonable steps to:

(i) secure the API and the API Key (including all copies thereof) from infringement, misappropriation, theft, misuse of unauthorised access; and

(ii) prevent the introduction of any Virus or Vulnerability into NCS's network and information systems (including NCS's hCRM), via the Customer's (or End User's) use of the API, the API Key or otherwise.

9. NCS's warranties

9.1 The API is provided to the Customer on an 'as is' basis.

9.2 Subject to clause 9.4, all warranties, representations, conditions and all other terms of any kind whatsoever implied by statute or common law are, to the fullest extent permitted by applicable law, excluded from API Terms.

9.3 Specifically, NCS:

(a) does not warrant that:

(i) the Customer's use of the API will be uninterrupted or error-free; or

(ii) the API will be free from Vulnerabilities or Viruses; and

(b) is not responsible for any delays, delivery failures, or any other loss or damage resulting from the transfer of data over communications networks and facilities, including the internet, and the Customer acknowledges that the API may be subject to limitations, delays and other problems inherent in the use of such communications facilities.

9.4 NCS warrants that it has and will maintain all necessary licences, consents, and permissions necessary for the performance of its obligations under these API Terms.

10. Limits of liability

10.1 Except as expressly and specifically provided in these API Terms, the Customer assumes sole responsibility for results obtained from the use of the API by the End Users and for conclusions drawn from such use. NCS shall have no liability for any damage caused by errors or omissions in any information, instructions or scripts provided to NCS by the Customer in connection with the API, or any actions taken by NCS at the Customer's direction.

10.2 NCS's liability under these API Terms shall be limited to the extent of the liability provisions in the Main Agreement, including without limitation the heads of losses and the total liability cap, save for any exclusions.

11. Intellectual property rights

11.1 The Customer acknowledges that all Intellectual Property Rights in the API, belong and shall belong to the NCS, and the Customer shall have no rights in or to the same other than the right to use it in accordance with these API Terms.

11.2 The Customer will promptly notify NCS if the Customer becomes aware of any infringement of any Intellectual Property Rights in the API and will fully co-operate with NCS in any legal action taken by the NCS to enforce NCS's Intellectual Property Rights.

12. Integration with the Main Agreement

API Terms shall be incorporated into and form part of the Main Agreement between the Parties.

13. Duration and termination

13.1 API Terms shall commence on the day the API is first used by the Customer. For the purposes of this clause, 'first use' shall mean the date and time when the Customer makes the first API Call or otherwise interacts with the API.

13.2 API Terms shall be effective and remain in force only for the duration of the Main Agreement. API Terms shall automatically terminate upon termination or expiration of the Main Agreement.

14. Conflict

In the event of any conflict or inconsistency between these API Terms and the Main Agreement, the provisions of the Main Agreement shall prevail, except to the extent that specific terms of API Terms explicitly amend or supplement the Main Agreement.

15. Governing law and jurisdiction

15.1 These API Terms and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by and construed in accordance with the law of England and Wales.

15.2 The parties irrevocably agree that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim that arises out of or in connection with API Terms or its subject matter or formation (including non-contractual disputes or claims).

ANNEX A API Key Security and Usage Compliance Form

We value your commitment to protecting sensitive information and ensuring the security of your assigned API Keys. Please complete the following form to confirm that you follow appropriate security practices and only use API Keys for registered applications.

1. Customer Information

- **Company Name**:
  ____
- **Contact Name**: ____
- **Email Address**: ____
- **Phone Number**: ____

2. Details of Customer Application

- **Name:____**
  ____
- **Optional: Technology Stack (e.g. Python, etc.) ______________**

3. API Key Storage & Security

Please confirm the following practices to ensure the security of your API Keys:

Statement	Yes

a. API Keys are stored securely using environment variables, encrypted databases, or secure vaults (e.g., AWS Secrets Manager, Azure Key Vault, etc.).	□
b. API Keys are never hardcoded in source code or configuration files that are exposed to the public.	□
c. Access to API Keys is limited to authorized personnel only.	□
d. Multi-factor authentication (MFA) is enabled for accounts that have access to the API Keys.	□
e. Logs that contain API Keys or sensitive information are either sanitized or protected using encryption.	□

4. API Key Usage

Please confirm that API Keys are used appropriately:

Statement	Yes
a. API Keys are only used by registered applications, and each application is registered with its own unique API key.	□
b. API Keys are not shared between applications or external third parties.	□
c. Applications using the API Keys implement IP whitelisting or similar access restrictions to prevent unauthorized use.	□
d. Access to API Keys is monitored, and usage is logged for audit purposes.	□
e. API requests are rate-limited to prevent system overload/overuse of resources.	□

5. Incident Response

Please confirm your incident response plan in case of compromised API Keys:

Statement	Yes
In case of a suspected API Key compromise, you have a process in place to notify NCS to revoke or rotate the Key immediately.	☐

6. Additional Comments

If there is anything else you'd like to provide or clarify, please do so below:

7. Confirmation

I confirm that the information provided above is accurate and that we follow the security and usage practices outlined in this form.

Name: ____

Title: ____

Date: ____

Signature: ________________________________