

# Auria's Atolli – Terms of Use

1.3.2023 (ENG)

## 1 Introduction

By using the secure operating environment produced by the Auria Clinical Informatics of the wellbeing services county of Southwest Finland (Varha) you accept the terms of use presented here and the information security practices in accordance with the privacy statement.

1. The wellbeing services county of Southwest Finland (Varha) Auria Clinical Informatics ("supplier") is responsible for producing and maintaining the service. / Tyks building 11 B PL 52, 20521 Turku.
2. The service's currently valid user instructions, prices, order and change order forms, the privacy statement and these terms of use can be found on the website of Auria Clinical Informatics [Auria Tietopalvelu - Atolli](#)
3. The service is a secure operating environment as referred to in § 20 of the Act on the Secondary Use of Social and Health data (552/2019), which meets the requirements set by Social and Health Data Permit Authority, Findata, regarding secure operating environments (REGULATION 1/ 2022).

## 2 Ordering and contract formation

4. Ordering ("order") the service ("secure operating environment") and changes to it are made using the order and change order forms provided by Auria Clinical Informatics, which are filled out in accordance with their internal instructions and delivered to Auria Clinical Informatics at the address [atolli@varha.fi](mailto:atolli@varha.fi). The persons for whom access to the secure operating environment is applied for are marked on the order or change order form. These persons are referred to below as users.

5. The party, which orders the service ("orderer"), is specified in the order form and can be an organization or a natural person. The orderer becomes a customer of Auria Clinical Informatics, and the contract ("contract") between the customer and Auria Clinical Informatics ("contracting parties") regarding the delivery of the service to the customer is created when the order placed by the customer has been accepted and confirmed by Auria Clinical Informatics with an order confirmation, which Auria Clinical Informatics sends by e-mail to the contact person of the order in question.
6. The order confirmation contains information about the customer, deliveries, price and delivery schedule.
7. The contract documentation consists of the order confirmation, these terms of use, and the privacy statement.
8. Auria Clinical Informatics accepts an order if the conditions for acceptance are met, and the information requested in the order or change order form is correctly filled in according to instructions with all necessary attachments. Auria Clinical Informatics has the right to refuse to accept an order if the order or change order form is incomplete or if there is no legal basis for the order.
9. When the order is accompanied by a data permit, only the data permit's licensee who is a natural person or the data permit licensee's contact person has the right to order the service, because that person is the only entity whose binding relationship with the licensee is defined in the data permit. If, during the validity of the data permit, this original contact person is no longer available to Auria Clinical Informatics and someone else tries to change the order or to end it on his behalf, it is not enough that the new person is one of the data processors mentioned in the data permit. For changes to the service, the new customer must be able to submit a data permit change decision to Auria Clinical Informatics, which indicates the new contact person. If a data permit change decision is not available, Auria Clinical Informatics' customer service representative requests a written confirmation from the organization of the contact person of the original data permit about a new contact person.

10. The orderer of the service has the obligation to notify Auria Clinical Informatics without delay of any changes to a data permit that affect the data, users or access rights processed in the service.
11. The orderer of the service must provide Auria Clinical Informatics sufficient and correct information for the delivery of the service and reasonably contribute to the delivery of the service. The orderer of the service is responsible for the information and instructions given to Auria Clinical Informatics and for updating them.
12. If desired, the contact person of the orderer has the option to install software in the ordered secure operating environment in accordance with the user instructions. In such case, the orderer is responsible for any possible license fees or costs, which might be required to use the additional installed software legally. The orderer's contact person can, if they wish, delegate the installation of the software to another person, which is entitled to process data in the secure operating environment according to the order confirmation/data permit. The orderer's contact person must then inform Auria Clinical informatics of this delegation by e-mail.
13. Use of the service is subject to a fee. The orderer is invoiced a monthly fee once (a) the secure operating environment related to the order has been established, (b) instructions for logging in have been sent to the users by e-mail, and (c) the data has been transferred to the ordered secure operating environment. The price of using the service consists of a monthly usage fee and possible one-time payments based on ordered additional services, which are invoiced separately.
14. The current prices can be found on the website of Auria Clinical Informatics. The prices are presented in euros and the invoicing currency is euro. The prices are presented without VAT, and VAT is added to the prices at the time of invoicing in accordance with the regulations in force at any given time. The minimum invoicing period is three (3) months and invoicing takes place every three (3) months. The payment term is 14 days net or by a separate agreement. Penalty interest is in accordance with the Interest Act.

15. The orderer of the service can terminate and end the order before the end date of the usage period of the secure operating environment indicated in the order confirmation, which is indicated in the section "The usage period of the environment begins/ends". In this case, the payment by to the minimum billing period that may have already been charged will not be refunded.
16. Auria Clinical Informatics confirms prices periodically and reserves the right to change prices. A possible price change will automatically come into effect for existing orders at the beginning of the billing period following the current billing period of each order.
17. Auria Clinical Informatics has the right to remove user rights if the orderer of the service fails to pay the invoice for the order despite reminders.

## 4 Transferring data to the service

18. Data is transferred to a secure operating environment by the process described in the user guide.
19. A user is not allowed or able to transfer data to or from the secure operating environment himself. Data is always transferred by Auria Clinical informatics. The software installed in the secure operating environment does not allow data to be transferred or sent out.
20. Data transferred to the service and processed in the service must have proper authorization or another legal basis. Auria Clinical Informatics has the right to refuse the transfer of data to the secure operating environment if Auria Clinical Informatics considers that there is no legal basis for delivering the data to the secure operating environment.
21. The orderer is responsible for ensuring that the data transferred to its secure operating environment is correct. If the orderer notices or suspects that the data transferred is incorrect or improper, one must immediately notify Auria Clinical Informatics customer service at [atolli@varha.fi](mailto:atolli@varha.fi)

## 5 Access rights and user login

22. The orderer of the service is responsible for ensuring that users have the right to process the project's data.
23. Users are granted access to the service.
24. Users log into their secure operating environments with Suomi.fi authentication in accordance with the process described in the user guide. Login usernames or passwords are not distributed to users.
25. Users are identified and authenticated with a strong two-step identification technology.
26. The access rights of the service follow the principle of least privilege. The maintenance access rights of the service, confidential information processed by Auria Clinical Informatics personnel or users, and all other information that must be limited in terms of visibility or access, are limited in accordance with the principle of least privileged access with access rights definitions and system handling rules.
27. Users' access rights in the service are at basic user level. In connection with the installation of additional programs, one user can be granted a temporary extended access right to their own environment.
28. Each project and its data is isolated to a project-specific secure operating environment. Only the users listed in a data permit are granted access to the secure operating environment implemented on the basis of that data permit and to the data located there.

29. If a person has access rights to several project-specific secure operating environments, the person is allowed to keep an open connection to these secure operating environments at the same time, but the transfer of data between the environments is prohibited and blocked at the operating system and software level.
30. The main users of Auria Clinical Informatics are the administrators of the secure operating environment and are the only ones who have access to its management and maintenance functions. Main users are prohibited from accessing data located in customer's secure operating environments.

## 6 Use of the service

31. A user must use the service in accordance with the terms of use and instructions for use.
32. A user can start using the secure user environment after the start of a first invoicing period of an order as described in section 13.
33. Direct data connections to the secure operating environment are not allowed from the user's terminal device or anywhere else. The use of the service takes place via data connection, with which only the screen image and keyboard and mouse input are transferred between the user's terminal device and the service.
34. A user guide produced by Auria Clinical Informatics is available to the user. Auria Clinical Informatics provides other support related to the service only if it has been separately agreed upon.
35. The orderer or any user of the service does not have the right to resell or otherwise distribute the service to any other third parties.

## 7 Locking out a user

- 36. The user's right to use and access to the secure operating environment is locked when the secure operating environment's use period or its project related data permit expires.
- 37. The user's access to the service is temporarily blocked if the user fails to identify three times in a row when logging in.
- 38. Auria Clinical Informatics can block the user's access to the secure operating environment if the user does not comply with the terms of use of the service, the user is found to be causing disturbances or is assessed as a threat to the service. In this case, the user and the orderer of the service will be informed.

## 8 Exporting the results derived from the data out of the secure operating environment

- 39. Outside the secure operating environment, the user may only use anonymous results derived from the data.
- 40. Data transfer out of the secure operating environment is always done by Auria Clinical Informatics. The user cannot move the data out himself.
- 41. Before exporting the data, the orderer commits to independently anonymize the material in accordance with Findata's instructions on how to [produce anonymous results](#) and after the data export to deliver the anonymized data to Findata for review.

## Closing the secure user environment and termination of the agreement

42. When the secure operating environment is closed, the contract between Auria Clinical Informatics and the orderer of the service ends.
43. The secure operating environment is closed when the usage period of the secure operating environment ends at the end date confirmed in the order confirmation. If the operating environment order is accompanied by a data permit, the secure operating environment will be closed at the latest when the data permit expires.
44. Closing the secure operating environment and terminating the service can be done at the request of the orderer's contact person before the end of the usage period. In this case, the orderer's contact person must make a change order regarding closing the environment.
45. Auria Clinical Informatics will keep an environment and its data for a maximum of six (6) months after the expiration of a data permit, after which the environment and its data will be deleted according to Findata's regulation, unless the law or the data permit stipulates otherwise. If the orderer of the service requests access to the data during the storage period of six (6) months, the orderer of the service must make a new order for the environment, in which case Auria Clinical Informatics will ensure that the orderer of the service and its users have a valid data permit to process the data.
46. Auria Clinical Informatics has the right to close the secure operating environment, if contrary use against the terms of use or other misuse occurs.

## 9 Data Protection



47. Auria Clinical Informatics collects and stores personal data as well as statutory technical and log information, which are described in the privacy statement.
48. The use of the service is only for the user's personal use. The user may not provide credentials to any other person intentionally or unintentionally or leave the terminal device unlocked while logged in to the service. The user must take care of the secure use and storage of the identification tools used for logging in. Log information is collected and stored from all data traffic that takes place in the service.
49. When processing data, users must ensure that confidential data is not passed on to third parties. Even if the data is pseudonymized, it must be kept secret during and after using the secure operating environment. It is forbidden to try to circumvent the protections included in the service in order to obtain non-aggregated data for the user's own terminal device or any data medium located outside the secure operating environment.

## 10 System integrity and security

50. Auria Clinical Informatics does not take responsibility for damages caused by technical or software errors or inappropriate use of resources.
51. Auria Clinical Informatics has the right to change the content, operation and accessibility of the service in order to develop the service or for any other necessary reason, without limitation, in the way and at the times it deems best. If the change significantly affects the content or service level of the software service, the supplier must notify the customer of the change in writing at least 90 days before the effective date of the change, and the customer has the right to terminate the contract with a 30-day notice period. The termination in question must be made in writing no later than 14 days after the effective date of the change.
52. If the user detects information security deficiencies, the user must report them to Auria Clinical Informatics. Information related to information security deficiencies may not be

disseminated. Searching for security weaknesses is not prohibited, but its goal must be to improve the service's data security, and Auria Clinical Informatics must be informed about it.

53. In all situations, users must follow responsible conduct of research and Finnish law.

## 11 General obligations

54. Auria Clinical Informatics is responsible for ensuring that the service is in accordance with the contract and that the tasks it is responsible for are carried out in accordance with the contract, carefully and with the professionalism required by the tasks. Auria Clinical Informatics immediately informs the customer of a matter that has come to their attention, which may prevent the use of the service in accordance with the contract.

55. The orderer of the service is responsible for ensuring that the tasks under its responsibility are carried out in accordance with the contract. The orderer of the service is responsible for acquiring the devices, data connections, software and costs they need to use the service and bringing the information systems in line with the service.

## 12 Procedure when misuse is detected

56. Upon detecting misuse or a strong suspicion of misuse, Auria Clinical Informatics will act without delay in such a way as to prevent the occurrence of damage or further damage. Depending on the case, the measures to minimize damages may be (a) limiting or removing user access rights, (b) temporarily closing secure operating environments or (c) starting a proper investigation process with Auria Clinical Informatics and, if necessary, with authorities.

## 13 Service production subcontractors

57. In order to provide the service, Auria Clinical Informatics acquires data center services from 2M-IT Oy as a subcontracting service, including servers, data network equipment and other necessary IT equipment.

## 14 Maintenance interruptions

58. Information security and data center technology related software is updated monthly as part of planned maintenance procedures. The maintenance window is held on the first Tuesday of every month at 17.00–07.00, which is implemented if the service provider estimates that there is a need for it. If a service interruption occurs, Auria Clinical Informatics will inform customers in advance of the upcoming service interruption on the service's public login page [Atolli](#).

59. Auria Clinical Informatics does not guarantee uninterrupted and flawless operation of the service. The service is checked regularly to prevent malfunctions. The service provider has the right to interrupt the operation of the service due to a change, reform, maintenance and installation work or a similar reason related to the service, or if required by legislation or other official order. However, the aim is to notify users of interruptions as early as possible.

## 15 Changes to terms of use

60. Auria Clinical Informatics has the right to change these terms for a justified reason. Changes will be announced on Auria Clinical Informatics' website and the users separately. Information will not be provided if the change to the terms is minor or of technical nature.

## 16 Obstacle force majeure

61. Auria Clinical Informatics is not responsible for delay or damage caused by an obstacle beyond its control, which cannot reasonably be expected and whose consequences it could not reasonably have avoided or overcome. A force majeure, unless otherwise shown, is considered to be, for example, war or rebellion, earthquake, flood or other comparable natural disaster, interruption of public telecommunications or public electricity distribution, import or export ban, strike, lockout, boycott or other comparable industrial action. A strike,

lockout, boycott, or other comparable industrial action is considered, unless otherwise shown, a force majeure also when Auria Clinical Informatics is itself the target or party to it.

62. A force majeure incident to Auria Clinical Informatics' subcontractor is also considered Auria Clinical informatics' force majeure.

## 17 Applicable law and dispute resolution

63. The contract is governed by Finnish law.

64. Disputes arising from the contract will be settled definitively in arbitration in accordance with the arbitration rules of the Central Chamber of Commerce. The dispute will be resolved by one arbitrator. The place of arbitration is Turku, and the arbitration is conducted in Finnish. However, a claim regarding a monetary claim can also be settled in the general court of the defendant's place of residence.