



Policy

**CLN-POL-0000049 Global Data Protection Policy**

**Effective Date:** 14-Feb-2023

DocuSigned by:

*AM*



Signer Name: Andreea Moldovanu  
 Signing Reason: I approve this document  
 Signing Time: 31-Jan-2023 | 4:15 PM GMT

E66126E6CAAB47169CFDFE780424B1C1

Author	Title:	Signature:	Date:
Hannah Jones	Legal Counsel	DocuSigned by: <i>Hannah Jones</i> Signer Name: Hannah Jones Signing Reason: I am the author of this document Signing Time: 31-Jan-2023   3:43 PM GMT 20C8CDB04A31452EBD44327276EDC45E	31-Jan-2023   3:44 PM GMT

Reviewer	Title:	Signature:	Date:
Mark Ashton-Blanksby	Director of Audit & ESG Programme Management	DocuSigned by: <i>Mark Ashton-Blanksby</i> Signer Name: Mark Ashton-Blanksby Signing Reason: I approve this document Signing Time: 31-Jan-2023   3:45 PM GMT A9C3474BE8DF4B29A92620948036808B	31-Jan-2023   3:45 PM GMT

Quality Approver	Title:	Signature:	Date:
Najma Ali	Responsible Person and Quality Manager	DocuSigned by: <i>Najma Ali</i> Signer Name: Najma Ali Signing Reason: I approve this document Signing Time: 31-Jan-2023   3:47 PM GMT 1901AB6C30DE4D2893D107ADF86BB79D	31-Jan-2023   3:47 PM GMT

**If this Policy is a printed copy it shall be considered an uncontrolled copy**

**TABLE OF CONTENTS**

1. Executive Summary ..... 3

2. Purpose..... 3

3. Scope ..... 3

4. Abbreviations and Definitions ..... 3

5. Data Protection Principles ..... 4

6. Policy Compliance and Maintenance ..... 8

7. Contact..... 8

8. ANNEX A ..... 9

9. Document History..... 10

## 1. Executive Summary

Clinigen Limited and any company, partnership or other person which directly or indirectly is controlled by Clinigen Limited (**'Clinigen'**) processes personal data relating to patients, healthcare practitioners (including physicians and pharmacists), customers, clients, contractors, reporters of adverse events, employees/former employees/recruitment applicants/consultants (**'Employees'**) and suppliers (referred to as **'Data Subject(s)'**).

Clinigen is committed to protecting the privacy of data subjects' Personal Data. Clinigen has, therefore, implemented a global data protection compliance program to ensure high standards for Clinigen's Data Processing of Personal Data. This Policy sets out the basis of this program and how Employees should manage Clinigen's data subjects' Personal Data.

## 2. Purpose

This Policy outlines our approach to data protection and the rights of data subjects in relation to their Personal Data. The Policy sets out the commitment made by Clinigen to:

- manage Personal Data;
- comply, and evidence on-going compliance, with applicable data protection laws, in the countries in which Clinigen operates;
- ensure that Personal Data is processed in accordance with data subjects' rights.

## 3. Scope

This Policy applies to all Clinigen Personal Data, regardless of whether it is in paper or electronic format. All Clinigen Employees are required to adhere to this Policy.

Clinigen shall comply with applicable Personal Data protection laws and requirements in the territories within it operates. This Policy applies to Clinigen globally, as well as certain additional requirements for territories Clinigen operates within where there is additional or differing data protection laws; please see the [Territory Requirements](#) for more information.

## 4. Abbreviations and Definitions

Key terms used within this Policy are defined in the table below:

Terms	Definition
Data Breach	An actual or suspected breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.
Data Controller	The person or organisation that determines when, why and how personal data is Data Processed. The Data Controller is responsible for establishing practices and policies in accordance with data protection law.
Data Processor	Any natural or legal person, public authority, agency or other body which Data Processes on behalf of a Data Controller.
Data Processing, Data Processed or Data Process	Any activity that involves the use of personal data. It includes obtaining, recording or holding the personal data, or carrying out any operation or set of operations on such data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Data Processing also includes transmitting or transferring Personal Data to third parties. In brief, it is anything that can be done to personal data from its creation to its destruction, including both creation and destruction.

**If this Policy is a printed copy it shall be considered an uncontrolled copy**

Terms	Definition
DPIA	Data Protection Impact Assessment.
Data subject(s)	Has the meaning given in paragraph 1 of this Policy.
Employee(s)	Has the meaning given in paragraph 1 of this Policy.
Personal Data	Any information relating to an identified or identifiable natural person.
ROPA	Record of Processing Activities

## 5. Data Protection Principles

### 5.1 Principles

Clinigen uses the following high-level principles to establish its practices for processing Personal Data:

- **Fairness:** Clinigen shall process Personal Data in a fair, lawful, legitimate, and transparent manner.
- **Purpose Limitation:** Clinigen shall only create or collect Personal Data for a specific, explicit, and legitimate purpose(s). Any subsequent processing shall be compatible with such purpose(s), unless Clinigen has obtained the individual's consent, or the processing is otherwise permitted by law.
- **Proportionality:** Clinigen shall only process Personal Data that is adequate, relevant, and not excessive for the purpose(s) for which it is processed.
- **Data Integrity:** Clinigen shall keep Personal Data accurate, complete, and up to date as is reasonably necessary for the purpose(s) for which it is processed.
- **Data Retention:** Clinigen shall keep Personal Data in a form that is personally identifiable for no longer than necessary to accomplish the purpose(s), or other permitted purpose(s), for which the Personal Data was obtained.
- **Data Security:** Clinigen shall implement appropriate and reasonable physical, technical, and organisational measures to safeguard Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure, use, or access.
- **Individual Rights:** Clinigen shall process Personal Data in a manner that respects data subjects' rights under applicable Personal Data protection laws.
- **Accountability:** Clinigen shall implement appropriate governance, policies, processes, controls, and other measures necessary to enable it to demonstrate that its processing of Personal Data is in accordance with this Policy and applicable Personal Data protection laws.

### 5.2 Clinigen's Responsibilities

#### 5.2.1 Related Policies, Procedures and Notices

In its role as Data Controller and/or Data Processor, Clinigen has established related policies and procedures in order to comply with data protection laws and regulations, which include:

- [Territory Requirements](#);
- [Employee Privacy Notice](#);
- [Clinigen Corporate Website Privacy Policy](#);
- [Website Cookies Policy](#);
- [Privacy Statement for Pharmacovigilance Data](#);
- [Information Security Policy](#);
- [Global Data Protection Governance Framework](#); and
- [Global Data Breach Management Procedure](#).

**If this Policy is a printed copy it shall be considered an uncontrolled copy**

### 5.2.2 Training

All Employees are required to read this Policy and the related policies, procedures and notices listed in paragraph 5.2.1 above. Certain Employees are required to complete competency training to enable them to comply with data protection requirements. Training completion rates will be monitored centrally.

### 5.2.3 Third Party Data Processors

When Clinigen is a Data Controller, Clinigen retains responsibility and oversight of all Data Processing activities, even when Data Processing is carried out by a third party, on behalf of Clinigen. Where applicable, Data Processing activities conducted by a third party Data Processor are recorded in Clinigen's ROPAs.

### 5.2.4 Record Keeping

Clinigen maintains ROPAs, using a data protection compliance platform called "ROBUS". The ROPAs are reviewed at least annually and will be reviewed more frequently in the event of any significant organisational or Data Processing activity changes to Clinigen, to ensure that the ROPAs accurately reflect Data Processing activities.

If a ROPA deems a Data Processing activity to be high risk, Clinigen shall complete a risk assessment called a DPIA (these are also known as 'Personal Information Impact Assessments' or 'Privacy Impact Assessments' in some jurisdictions). A DPIA describes the purpose of the Data Processing, and includes an assessment of:

- the necessity and proportionality of the Data Processing;
- the potential risk to data subjects, as a result of the Data Processing; and
- any risk-mitigation to reduce the risks identified for data subjects.

Employees should complete a risk assessment as a pre-requisite to any new process or project that involves Data Processing and/or any significant change to an existing process or project involving Data Processing. DPIAs are completed using ROBUS and are approved by a member of the Data Protection Compliance Board. Please see the Global Data Protection Governance Framework and/or any applicable Territory Requirements for further information.

## 5.3 Sensitive Personal Data and Children's Data

Clinigen recognises that some personal data requires additional protection, because it is particularly sensitive in nature. Any processing of sensitive personal data should be documented in a ROPA(s) and a risk assessment completed in ROBUS by the relevant Employee that owns the process utilising the sensitive personal data.

### 5.3.1 Sensitive personal data

Personal Data regulations and laws often refer to 'special category' or 'sensitive' personal data which is a form of personal data which is sensitive in nature. Examples of sensitive personal data are:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data or biometric data (for the purposes of identification);
- Health information; and
- Information regarding an individual's sex life or sexual orientation.

Clinigen may process sensitive data, as part of checking patient eligibility, within Clinigen's Managed Access business, or reporting adverse events, within Clinigen's Pharmacovigilance or Medical Information functions.

### 5.3.2 Children's personal data

Children's personal data requires additional protection because children are vulnerable and less aware of data protection risks. Overall, Clinigen has limited exposure to the processing of children's personal data, however, in the instances where Clinigen does process children's personal data, Clinigen documents this in a ROPA and communicates to the parent(s) or guardian(s) via privacy notices.

## 5.4 Data Processing Basis

### 5.4.1 Lawful Basis

There are six possible lawful bases for Data Processing:

- The data subject has provided clear consent for Clinigen to Data Process their Personal Data;
- The Data Processing is necessary for a contract which Clinigen has with the data subject;
- The Data Processing is necessary for Clinigen to comply with the law;
- The Data Processing is necessary to protect an individual's life;
- The Data Processing is necessary for Clinigen to perform a task in the public interest; or
- Clinigen has a legitimate interest to Data Process a data subject's Personal Data, unless there is a good reason to protect the Personal Data which overrides those legitimate interests.

Clinigen has documented the most appropriate lawful basis for each Data Processing activity in the relevant ROPA(s). If an Employee is implementing a new Data Processing activity, or a change to an existing Data Processing activity, they will need to determine the lawful basis of Data Processing for the activity. Please contact the Legal team for assistance.

### 5.4.2 Consent

Employees should contact the Legal team for assistance if you are implementing a new Data Processing activity or a change to an existing Data Processing activity that relies upon data subjects' consent. If Clinigen wishes to rely on a data subjects' consent to process their Personal Data, the Employee(s) that own the Data Processing activity must ensure that:

- Consents constitute a documented, positive indication of the data subjects' wishes (i.e., an opt-in, not an opt-out); and
- There is a robust consent management process embedded that enables Clinigen to continually track and update captured consents as required.

Data subjects have the right to withdraw their consent at any time, therefore Clinigen must ensure that Data Processing activity ceases if a consent is withdrawn, although it should be noted that if individuals withdraw their consent, Clinigen may not be able to provide certain products or services.

### 5.4.3 Legitimate Interests

As legitimate interest is the most flexible lawful basis, any Data Processing activity that relies on this basis must include a 'Legitimate Interest Assessment', to justify the use of this lawful basis.

Legitimate Interest Assessments are linked to each Data Processing activity in a ROPA on ROBUS. These will be reviewed and updated as and when required to ensure they remain accurate and up to date.

## 5.5 International Transfers of Personal Data

Employees should be aware there where personal data is transferred outside of country, data protection laws in certain jurisdictions require additional safeguards to be implemented to ensure that the level of protection afforded to data subjects' personal data is not undermined. Clinigen will need to document any exposure to international transfers of personal data in the relevant ROPA(s).

Please see the relevant Territory Requirements for more information on international transfers and any queries regarding international transfers of Personal Data should be directed to the Legal team.

## 5.6 Data Subject's Rights

Depending on their location, data subjects may have rights in relation to the way Clinigen processes their Personal Data, which include the following:

- **The right to be informed of data processing activity** - this is usually achieved by privacy notices, such as Clinigen's website or employee privacy notices.
- **The right of access, also known as a subject access request** - this enables data subjects to request a confirmation of whether Clinigen processes their Personal Data, and if it does, to obtain a copy of their Personal Data.
- **The right to rectification** - this enables data subjects to request rectification of inaccurate or incomplete Personal Data held for the data subject.
- **The right to erasure** - this enables data subjects to request deletion of their Personal Data.
- **The right to restrict data processing** - this can be requested in specific circumstances.
- **The right to data portability** - data subjects have the right in certain jurisdictions to request that their Personal Data is transferred to a third party in a structured, commonly used, and machine-readable format.
- **The right to object** - to the processing of a data subject's Personal Data.
- **Rights in relation to Automated Decision Making** - this is the right for a data subject not to be subject to decisions based solely on Automated Decision Making.

Where Clinigen receives a request from a data subject relating to the rights listed above it will have certain time frames it must respond within. Where Clinigen is acting as a Data Controller the relevant regulatory authority will determine the response time, for example in the UK Clinigen would have one month from receipt of the original request to respond, and in some scenarios, this can be extended by a further two months. Where Clinigen is acting as a Data Processor on behalf of a third-party Data Controller, Clinigen must notify the Data Controller of the request in accordance with Clinigen's contract with the Data Controller.

Data subjects also may have the right to lodge a complaint with the relevant supervisory authority, if they feel that their Personal Data has not been processed in line with data protection regulations.

Clinigen has developed internal procedures which govern the process an Employee should follow; in the event a data subject access request is received – please see the Annex A to this Policy for more information. If an Employee receives a data subject rights request, please contact the Legal team immediately.

## 5.7 Data Breach Management

Clinigen maintains complete oversight of all Data Breaches globally. All Clinigen Employees who suspect that a Data Breach may have occurred must report the Data Breach immediately, via the online Data Breach Reporting Form, available on the [Clinigen Connect Homepage](#).

The Global Data Breach Management Procedure governs the process Employees should follow in the event of a Data Breach.

**If this Policy is a printed copy it shall be considered an uncontrolled copy**

Employees should be aware that time is of the essence in the event of a Data Breach:

- In instances where Clinigen is acting as a Data Controller in certain territories:
  - Clinigen may be required to report certain types of Data Breaches to the relevant supervisory authority within as little as 72 hours of discovery of the breach (where there is a high risk to the rights and freedoms of the affected data subjects, or a large number of data subjects are affected); and/or
  - Some types of Data Breaches must also be reported directly to the affected data subjects without delay.
- Where Clinigen is acting as a Data Processor in certain territories, it is required to notify the Data Controller of the Personal Data, as soon as possible in accordance with the relevant contract with the Data Controller and/or relevant data protection regulations.

## 6. Policy Compliance and Maintenance

### 6.1 Ensuring Compliance

Please see Clinigen's [Data Protection Governance Framework](#) for more information on how Clinigen ensures compliance with this Policy and the relevant roles that enable it to do so.

### 6.2 Compliance Measurement

Compliance with this will be monitored and verified by various means, including reports from available business tools, internal and external audits, self-assessment, and/or feedback to the Policy owner(s). Clinigen will periodically verify that this Policy continues to conform to applicable Personal Data laws and regulations.

### 6.3 Non-compliance

Deviations or non-compliance with this Policy, including attempts to circumvent the stated processes by bypassing or knowingly manipulating a process, system, or Personal Data may result in disciplinary action, including termination, civil action and lawsuits, and referral for criminal prosecution as allowed by local laws.

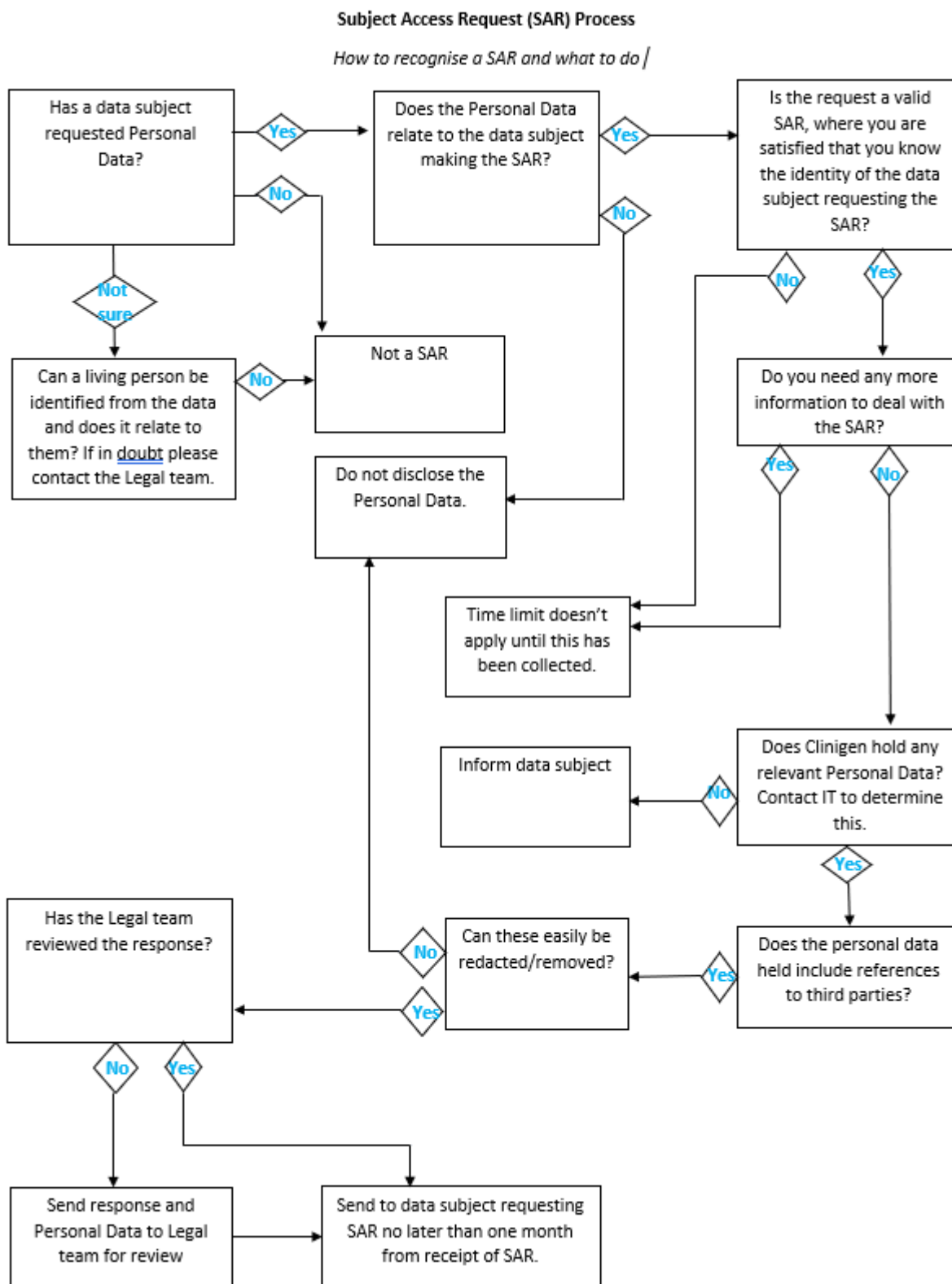
In some countries, violations of regulations designed to protect Personal Data may result in administrative sanctions, penalties, claims for compensation or injunctive relief, and/or other civil or criminal prosecution and remedies against Clinigen and culpable persons in their individual capacity.

## 7. Contact

Any questions in relation to this Policy should be directed to [Legal&Contracts@clingengroup.com](mailto:Legal&Contracts@clingengroup.com)




8. ANNEX A



If this Policy is a printed copy it shall be considered an uncontrolled copy

## 9. Document History

Change No.	Change Description (include previous policy reference if available)	Effective Date
01	New Global Data Protection Policy	14-Feb-2023  DocuSigned by: <i>AM</i>  Signer Name: Andreea Moldovanu Signing Reason: I approve this document Signing Time: 31-Jan-2023   4:16 PM GMT E66126E6CAAB47169CFDFE780424B1C1


**Certificate Of Completion**

Envelope Id: E7195385A2E142BF9CF5C4AD42307E89	Status: Completed
Subject: Please DocuSign CLN-POL-0000049 Global Data Protection Policy	
Source Envelope:	
Document Pages: 10	Signatures: 3
Certificate Pages: 5	Initials: 2
AutoNav: Enabled	Envelope Originator:
Envelopeld Stamping: Disabled	Andreea Moldovanu
Time Zone: (UTC) Dublin, Edinburgh, Lisbon, London	Pitcairn House
	Burton-on-Trent, NA DE14 2WW
	andreea.moldovanu@clinigengroup.com
	IP Address: 185.81.100.7


**Record Tracking**

Status: Original	Holder: Andreea Moldovanu	Location: DocuSign
1/25/2023 3:12:58 PM	andreea.moldovanu@clinigengroup.com	

**Signer Events**

Signer Events	Signature	Timestamp
Hannah Jones hannah.jones@clinigengroup.com Security Level: Email, Account Authentication (Required)	  Signature Adoption: Pre-selected Style Signature ID: 20C8CDB0-4A31-452E-BD44-327276EDC45E Using IP Address: 94.11.182.35  With Signing Authentication via DocuSign password With Signing Reasons (on each tab): I am the author of this document	Sent: 1/25/2023 3:19:43 PM Viewed: 1/31/2023 8:42:30 AM Signed: 1/31/2023 3:44:02 PM

**Electronic Record and Signature Disclosure:**  
Accepted: 1/31/2023 8:42:30 AM  
ID: 78a4b4ec-876b-48f0-97d2-ad762de081a9

Mark Ashton-Blanksby mark.ashton-blanksby@clinigengroup.com Head of Risk, Assurance & ESG Clinigen Limited Security Level: Email, Account Authentication (Required)	  Signature Adoption: Pre-selected Style Signature ID: A9C3474B-E8DF-4B29-A926-20948036808B Using IP Address: 86.153.197.239  With Signing Authentication via DocuSign password With Signing Reasons (on each tab): I approve this document	Sent: 1/31/2023 3:44:06 PM Viewed: 1/31/2023 3:44:46 PM Signed: 1/31/2023 3:45:18 PM
---	---	--

**Electronic Record and Signature Disclosure:**  
Not Offered via DocuSign

Signer Events	Signature	Timestamp
<p>Najma Ali  najma.ali@clinigengroup.com  Responsible Person  Clinigen Group Plc  Security Level: Email, Account Authentication (Required)</p>	<p><i>Najma Ali</i></p> <p>Signature Adoption: Pre-selected Style  Signature ID:  1901AB6C-30DE-4D28-93D1-07ADF86BB79D  Using IP Address: 89.197.193.210</p> <p>With Signing Authentication via DocuSign password  With Signing Reasons (on each tab):  I approve this document</p>	<p>Sent: 1/31/2023 3:45:22 PM  Viewed: 1/31/2023 3:47:30 PM  Signed: 1/31/2023 3:47:41 PM</p>

**Electronic Record and Signature Disclosure:**  
Not Offered via DocuSign

<p>Andreea Moldovanu  andreea.moldovanu@clinigengroup.com  Quality Administrator  Security Level: Email, Account Authentication (Required)</p>	<p><i>Andreea Moldovanu</i></p> <p>Signature Adoption: Pre-selected Style  Signature ID:  E66126E6-CAAB-4716-9CFD-FE780424B1C1  Using IP Address: 51.194.229.130</p> <p>With Signing Authentication via DocuSign password  With Signing Reasons (on each tab):  I approve this document  I approve this document</p>	<p>Sent: 1/31/2023 3:47:45 PM  Viewed: 1/31/2023 4:15:03 PM  Signed: 1/31/2023 4:16:28 PM</p>
--	--	---

**Electronic Record and Signature Disclosure:**  
Not Offered via DocuSign

In Person Signer Events	Signature	Timestamp
-------------------------	-----------	-----------

Editor Delivery Events	Status	Timestamp
------------------------	--------	-----------

Agent Delivery Events	Status	Timestamp
-----------------------	--------	-----------

Intermediary Delivery Events	Status	Timestamp
------------------------------	--------	-----------

Certified Delivery Events	Status	Timestamp
---------------------------	--------	-----------

Carbon Copy Events	Status	Timestamp
--------------------	--------	-----------

Witness Events	Signature	Timestamp
----------------	-----------	-----------

Notary Events	Signature	Timestamp
---------------	-----------	-----------

Envelope Summary Events	Status	Timestamps
-------------------------	--------	------------

Envelope Sent	Hashed/Encrypted	1/25/2023 3:19:43 PM
Certified Delivered	Security Checked	1/31/2023 4:15:03 PM
Signing Complete	Security Checked	1/31/2023 4:16:28 PM
Completed	Security Checked	1/31/2023 4:16:28 PM

Payment Events	Status	Timestamps
----------------	--------	------------

Electronic Record and Signature Disclosure
--

## **ELECTRONIC RECORD AND SIGNATURE DISCLOSURE**

From time to time, CLINIGEN GROUP (we, us or Company) may be required by law to provide to you certain written notices or disclosures. Described below are the terms and conditions for providing to you such notices and disclosures electronically through the DocuSign system. Please read the information below carefully and thoroughly, and if you can access this information electronically to your satisfaction and agree to this Electronic Record and Signature Disclosure (ERSD), please confirm your agreement by selecting the check-box next to 'I agree to use electronic records and signatures' before clicking 'CONTINUE' within the DocuSign system.

### **Getting paper copies**

At any time, you may request from us a paper copy of any record provided or made available electronically to you by us. You will have the ability to download and print documents we send to you through the DocuSign system during and immediately after the signing session and, if you elect to create a DocuSign account, you may access the documents for a limited period of time (usually 30 days) after such documents are first sent to you. After such time, if you wish for us to send you paper copies of any such documents from our office to you, you will be charged a \$0.00 per-page fee. You may request delivery of such paper copies from us by following the procedure described below.

### **Withdrawing your consent**

If you decide to receive notices and disclosures from us electronically, you may at any time change your mind and tell us that thereafter you want to receive required notices and disclosures only in paper format. How you must inform us of your decision to receive future notices and disclosure in paper format and withdraw your consent to receive notices and disclosures electronically is described below.

### **Consequences of changing your mind**

If you elect to receive required notices and disclosures only in paper format, it will slow the speed at which we can complete certain steps in transactions with you and delivering services to you because we will need first to send the required notices or disclosures to you in paper format, and then wait until we receive back from you your acknowledgment of your receipt of such paper notices or disclosures. Further, you will no longer be able to use the DocuSign system to receive required notices and consents electronically from us or to sign electronically documents from us.

### **All notices and disclosures will be sent to you electronically**

Unless you tell us otherwise in accordance with the procedures described herein, we will provide electronically to you through the DocuSign system all required notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you during the course of our relationship with you. To reduce the chance of you inadvertently not receiving any notice or disclosure, we prefer to provide all of the required notices and disclosures to you by the same method and to the same address that you have given us. Thus, you can receive all the disclosures and notices electronically or in paper format through the paper mail delivery system. If you do not agree with this process, please let us know as described below. Please also see the paragraph immediately above that describes the consequences of your electing not to receive delivery of the notices and disclosures electronically from us.

### **How to contact CLINIGEN GROUP:**

You may contact us to let us know of your changes as to how we may contact you electronically, to request paper copies of certain information from us, and to withdraw your prior consent to receive notices and disclosures electronically as follows:

To contact us by email send messages to: [jake.scothern@clinigengroup.com](mailto:jake.scothern@clinigengroup.com)

### **To advise CLINIGEN GROUP of your new email address**

To let us know of a change in your email address where we should send notices and disclosures electronically to you, you must send an email message to us at [jake.scothern@clinigengroup.com](mailto:jake.scothern@clinigengroup.com) and in the body of such request you must state: your previous email address, your new email address. We do not require any other information from you to change your email address.

If you created a DocuSign account, you may update it with your new email address through your account preferences.

### **To request paper copies from CLINIGEN GROUP**

To request delivery from us of paper copies of the notices and disclosures previously provided by us to you electronically, you must send us an email to [jake.scothern@clinigengroup.com](mailto:jake.scothern@clinigengroup.com) and in the body of such request you must state your email address, full name, mailing address, and telephone number. We will bill you for any fees at that time, if any.

### **To withdraw your consent with CLINIGEN GROUP**

To inform us that you no longer wish to receive future notices and disclosures in electronic format you may:

- i. decline to sign a document from within your signing session, and on the subsequent page, select the check-box indicating you wish to withdraw your consent, or you may;
- ii. send us an email to [jake.scothern@clinigengroup.com](mailto:jake.scothern@clinigengroup.com) and in the body of such request you must state your email, full name, mailing address, and telephone number. We do not need any other information from you to withdraw consent.. The consequences of your withdrawing consent for online documents will be that transactions may take a longer time to process..

### **Required hardware and software**

The minimum system requirements for using the DocuSign system may change over time. The current system requirements are found here: <https://support.docusign.com/guides/signer-guide-signing-system-requirements>.

### **Acknowledging your access and consent to receive and sign documents electronically**

To confirm to us that you can access this information electronically, which will be similar to other electronic notices and disclosures that we will provide to you, please confirm that you have read this ERSD, and (i) that you are able to print on paper or electronically save this ERSD for your future reference and access; or (ii) that you are able to email this ERSD to an email address where you will be able to print on paper or save it for your future reference and access. Further, if you consent to receiving notices and disclosures exclusively in electronic format as described herein, then select the check-box next to ‘I agree to use electronic records and signatures’ before clicking ‘CONTINUE’ within the DocuSign system.

By selecting the check-box next to ‘I agree to use electronic records and signatures’, you confirm that:

- You can access and read this Electronic Record and Signature Disclosure; and
- You can print on paper this Electronic Record and Signature Disclosure, or save or send this Electronic Record and Disclosure to a location where you can print it, for future reference and access; and
- Until or unless you notify CLINIGEN GROUP as described above, you consent to receive exclusively through electronic means all notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you by CLINIGEN GROUP during the course of your relationship with CLINIGEN GROUP.