2022

PAIA Manual of Medpace South Africa Pty. Ltd.

PREPARED IN ACCORDANCE WITH SECTION 51 OF THE PROMOTION OF ACCESS TO INFORMATION ACT, NUMBER 2 OF 2000 (“PAIA ACT”)

STEPHEN P. EWALD, INFORMATION OFFICER

Table of Contents

I. Background: Promotion of Access to Information Act ("PAIA")

PAIA was enacted on 3 February 2000, giving effect to the constitutional right in terms of section 32 of the Bill of Rights contained in the Constitution of the Republic of South Africa 108 of 1996 (the "Constitution") of access to any information held by the state and any information that is held by another person and that is required for the exercise or protection of any rights. In this PAIA Manual, all references to "sections" are to the Promotion of Access to Information Act, 2000 unless otherwise specified.

The purpose of PAIA is to promote the right of access to information, by transparently describing the right to information that is required for the exercise or protection of any right; and to actively promote a society in which the people of South Africa have effective access to information to enable them to exercise and protect their rights. In furtherance of these goals, under Section 51 of the Act, all Private Bodies are required to compile an Information Manual ("Manual").

PAIA establishes certain statutory rights of requesters to access records of a private body if:

- The records are required for the exercise or protection of any rights;
- The requester complies with all the procedural requirements; and
- Access to the record(s) is not refused in terms of any ground referred to in the PAIA.

Where a request is made in terms of the Act, the body to whom the request is made is obliged to release the information, subject to applicable legislative and / or regulatory requirements, except where the Act expressly provides that the information may be adopted when requesting information from a public or private body.

Under Section 17 of the Protection of Personal Information Act, No. 4 of 2013 ("POPI Act", together with PAIA, collectively "Acts"), a responsible party must maintain the documentation of all processing operations under its responsibility in a PAIA Manual. The POPI Act seeks to give effect to the constitutional right to privacy as contained in section 14 of the Bill of Rights and regulates the manner in which personal information may be processed by public and private bodies. In terms of POPI Act, the Information Regulator is responsible to regulate compliance with PAIA and its regulations by private and public bodies.

The Acts recognize that the right to access information cannot be unlimited and should be subject to justifiable limitations, including, but not limited to:

- Limitations aimed at the reasonable protection of privacy;
- Commercial confidentiality; and
- Effective, efficient and good governance;

This Manual is available for inspection:

- On the Medpace website at www.Medpace.com
- Upon reasonable request at our office located at 6 Griswold Road, Saxonwold, Johannesburg 2196 South Africa during normal business hours; or

- Upon written request from our Information Officer at 5375 Medpace Way, Cincinnati, Ohio 45227 USA or Privacy@Medpace.com.

This Manual will be updated from time to time, as and when required, without prior notice.

II. Information about Medpace and contact details for the Information Officer and Deputy Information Officer

Medpace Inc. is a global, full-service, Contract Research Organization (CRO) which conducts clinical trials on behalf of the pharmaceutical and medical device companies sponsoring the trials. The mission statement of Medpace, Inc. and its Affiliates ("Medpace") asserts that Medpace "emphasizes an uncompromising commitment to clinical research and to the highest level of ethical standards and performance in our jobs". A crucial component of this mission is the protection of confidentiality of study participants, and the adherence to all applicable data security and data privacy laws. Medpace states publicly that its governing principles include "honesty, confidentiality, integrity, and adherence to Medpace policies, standard operation procedures (SOPs) and applicable regulatory guidelines". This Manual is intended to demonstrate to sponsors, business partners, study subjects, auditors, and regulatory authorities that Medpace is living its mission and values, as reflected in a commitment to data security and data privacy at all levels of operations.

Medpace attempts to collect only as much personal data as needed to accomplish the purpose for which the information is collected, as determined by the Protocol. As agreed with the Sponsor (who as the Data Controller is ultimately responsible for determining the handling of clinical trial personal data) Medpace will securely dispose of records containing personal data so that the information cannot be read or reconstructed after it is no longer needed to comply with business purposes or legal obligations. This may involve the destruction of the pseudonymization key, purging of databases, physical destruction of hard copies, or other mechanisms.

Information Officer	**Stephen P. Ewald, General Counsel**
	Privacy@medpace.com
	+1 (513) 579-9911
	5375 Medpace Way, Cincinnati Ohio 45227 USA
Deputy Information Officer	**Carolyn Glashagan**
	Privacy@medpace.com
	6 Griswold Road, Saxonwold, Johannesburg 2196 South Africa

III. Overview of records held by Medpace

The information contained in this section is intended to identify the main categories of records held by Medpace and to help the requester to gain a better understanding of the main business activities of Medpace Further assistance in identifying the records held by Medpace is obtainable from the Information Officer.

IV. Records automatically available to the public [section 51(1)(b)(ii)]

No notice has been published pursuant to Section 51(1)(b)(ii), regarding the categories of records which are automatically available without having to request access in terms of PAIA.

V. Records held in accordance with other legislation [section 51(1) (d)]

Records from clinical trial participants are held in Medpace's proprietary clinical trial management software, ClinTrak ™. Guidance from clinical trial regulators, such as the US Food and Drug Agency, regarding compliance with 21 CFR Part 11 states that it is important to maintain an audit trail (along with other physical, logical, and security measures) to ensure "trustworthiness and reliability of records". Due to the high level of security and access control inherent to ClinTrak and study archives, the risk to individuals from having personal data retained in a ClinTrak audit trail is very low. Additionally, the regulatory and scientific reasons for maintaining a complete audit trail outweigh the risk of potential exposure. Therefore we do not recommend deleting personal data from the audit trail, even if entered in error.

Where applicable to its operations, Medpace also retains other records and necessary to its corporate functions. Unless disclosure is prohibited by applicable legislation, regulations, contractual agreements or otherwise, records that are required to be made available in terms of these acts shall be made available for inspection by interested parties in terms of the requirements and conditions of the Act. A request to access must be done in accordance with the prescriptions of the Act.

It is possible that this list may be incomplete. Whenever existing or new legislation allows a Requester access to records on a basis other than as set out here, this list shall be updated accordingly. Such updates may be made without notice.

Note that records will be provided only in accordance with the requirements stipulated in the relevant pieces of legislation. If a requester believes that a right to access to a record exists in terms of the legislation above, or any other legislation, the requester is required to indicate what legislative right the request is based on, to allow the Information Officer the opportunity to consider the request in light thereof.

VI. Records to which access will be provided in accordance with the PAIA

The accessibility of any records may be subject to the grounds of refusal set out in the Acts, and/or in this PAIA Manual. Amongst other reasons, records deemed confidential on the part of a third party will necessitate permission from the third party concerned, in addition to normal requirements, before Medpace will consider granting access to the requestor.

Category	Type of Documents
Company Records	Documents of incorporation
Financial Records	Annual Financial Statements Tax Returns Accounting Records
Personnel / Employee Documents and Records	Employment contracts Disciplinary records Salary records Leave records Training records Employee benefits arrangements rules and records
Vendor Management	Contractor, client and supplier agreements
Clinical Trial Records	Contracts Materials Transfer Agreements Regulatory Approvals

VII. Access Requests

The requester must comply with all the procedural requirements contained in the Act and this PAIA Manual relating to the request for access to a record, including completion and submission of an Access Request Form if required. The requester must complete any prescribed form attached as an Annex to this Manual (as may be updated from time to time), and submit any required fee and a deposit (if applicable)to the Information Officer or the Deputy Information Officer at the postal or physical address, or electronic mail address as noted above.

The request, including any prescribed form, must be filled in with sufficient information to enable the Information Officer to identify the record or records requested and the identity of the requester.

Proof of identity is required to authenticate the identity of the requester – in addition to any Access Request Form, requesters may be required to supply a certified copy of their identification document or a valid passport document, or if a legal entity, a certified copy of their Company Registration Certificate. The nature of information requested is at the sole discretion of the Information Officer for the purpose of authenticating the identity of the requestor.

The requester should indicate which form of access is required and specify a postal address, email address or fax number of the requester. The requester must state that he/she requires the information in order to exercise or protect a right, and clearly state what the nature of the right is so to be exercised or protected. The requester must clearly specify why the record is necessary to exercise or protect such a right (section 53(2)(d)).

If an individual is unable to complete the prescribed form because of illiteracy or disability, such a person may make the request by telephone or other mechanism.

If a request is made on behalf of another person, then the requester must submit proof of the capacity in which the requester is making the request to the reasonable satisfaction of the Information Officer (section 53(2)(f)).

Please note that the successful completion and submission of an Access Request Form does not automatically allow the requester access to the requested record. An application for access to a record is subject to certain limitations if the requested record falls within a certain category as specified in this Manual, which shall be determined at the discretion of the Information Officer.

The Information Officer will process the request within 30 (thirty) days, unless the requester has stated special reasons to the satisfaction of the Information Officer that circumstances dictate that the above time periods not be complied with. Failure to provide the required information in this section will result in a delay until the required information is provided. The prescribed time periods will not commence until the requester has furnished all the necessary and required information. The Information Officer will, within the prescribed 30 (thirty) days decide whether to grant or decline the request and give notice with reasons (if required) to that effect. The requester shall be advised whether access is granted or denied in writing. If, in addition, the requester requires the reasons for the decision in any other manner, the requester will be obliged to state which manner and the particulars required. This 30 (thirty) day period may be extended for a further period of not more than 30 (thirty) days, if the request is for a large volume of information, or the request requires a search for information held at other offices of one or more of Medpace, and the information cannot reasonably be obtained within the original 30 (thirty) day period. The requester will be notified in writing should an extension be sought.

The Information Officer shall redact a record, if possible, and grant only access to that portion requested and which is not prohibited from being disclosed.

All requests for information will be assessed on their own merits and in accordance with the applicable legal principles and legislation.

If a requested record cannot be found or if the record does not exist, the Information Officer shall, by way of an affidavit or affirmation, notify the requester that it is not possible to give access to the requested record. Such a notice will be regarded as a decision to refuse a request for access to the record concerned for the purpose of the Act. If the record should later be found, the requester shall be given access to the record in the manner stipulated by the requester in the prescribed form, unless the Information Officer refuses access to such record.

VIII. Refusal of Access to records (Chapter 4)

The Information Officer may refuse to provide access to records for any legal reason, in his or her sole discretion. The main grounds for refusal of a request for information are (but are not limited to):

- Mandatory protection of the privacy of a third party who is a natural person, which would involve the unreasonable disclosure of personal information of that natural person;
- Mandatory protection of the commercial information of a third party, if the record contains Trade secrets of that party;
- Financial, commercial, scientific or technical information which disclosure could likely cause harm to the financial or commercial interests of that party;
- Information disclosed by a third party to any of MEDPACE if the disclosure could put that third party at a disadvantage in negotiations or commercial competition;

- Mandatory protection of confidential information of third parties if it is protected in terms of any agreement – the provisions of the PAIA to apply in relation to the rights of the relevant third parties;
- Mandatory protection of the safety of individuals and the protection of property;
- Mandatory protection of records which could be regarded as privileged in legal proceedings;
- The commercial activities of the Companies, which may include (i) Trade secrets of the Companies; and (ii) Financial, commercial, scientific or technical information which, if disclosed, would likely cause harm to the financial or commercial interests of the Companies.
- Requests for information that are clearly frivolous or vexatious, or which involve an unreasonable diversion of resources shall be refused.

IX. Appeal from a refusal to grant access

The decision made by the Information Officer is final. If a requester is aggrieved by the refusal of the Information Officer to grant a request for a record, the requester may, upon notification of the Information Officer's decision (or upon deemed refusal in terms of Section 58 of the PAIA), lodge a complaint to the Information Regulator or apply to court for appropriate relief within the timeframes as prescribed by the PAIA.

X. Personal Information processed by Medpace

Chapter 3 of POPIA provides for the minimum Conditions for Lawful Processing of Personal Information by a Responsible Party. These conditions may not be derogated from unless specific exclusions apply as outlined in POPIA. The purpose for which personal information is processed by Medpace will depend on the nature of the information. In general, personal information is processed by Medpace for business administration purposes, including:

- To carry out actions for the conclusion or performance of a contract;
- To comply with obligations imposed by law;
- To protect the legitimate interests of the data subjects; or
- Where it is necessary for pursuing the legitimate interests of Medpace.

Medpace processes Personal Information relating to both individual and juristic persons in order to carry out its business and organizational functions. The manner in which this information is processed and the purpose for which it is processed is determined by Medpace. Medpace is accordingly a Responsible Party for the purposes of POPIA and will ensure that the Personal Information of a Data Subject:

- is processed lawfully, fairly and transparently. This includes the provision of
- appropriate information to Data Subjects when their data is collected by Medpace, in
- the form of privacy or data collection notices. Medpace must also have a legal basis (for
- example, consent) to process Personal Information;
- is processed only for the purposes for which it was collected;
- will not be processed for a secondary purpose unless that processing is compatible
- with the original purpose.
- is adequate, relevant and not excessive for the purposes for which it was collected;

- is accurate and kept up to date;
- will not be kept for longer than necessary;
- is processed in accordance with integrity and confidentiality principles; this
- includes physical and organizational measures to ensure that Personal Information,
- in both physical and electronic form, are subject to an appropriate level of security
- when stored, used and communicated by Medpace, in order to protect against access
- and acquisition by unauthorized persons and accidental loss, destruction or
- damage; and
- is processed in accordance with the rights of Data Subjects, where applicable.

Data Subjects have the right:

- To be notified that their Personal Information is being collected by Medpace;
- To be notified in the event of a data breach;
- To know whether Medpace holds Personal Information about them; and
- To access that information held by Medpace.
- To request the correction or deletion of inaccurate, irrelevant, excessive, out of date, incomplete, misleading or unlawfully obtained personal information;
- To object to Medpace's use of their Personal Information and request the deletion of such Personal Information (subject to Medpace record keeping requirements);
- To object to the processing of Personal Information for purposes of direct marketing by means of unsolicited electronic communications; and
- To complain to the Information Regulator regarding an alleged infringement of any of the rights protected under POPI and to institute civil proceedings regarding the alleged non-compliance with the protection of his, her or its personal information.

XI. Categories of Data Subjects and Personal Information [Section 51(1) (C) (Ii)]

As prescribed by Section 1 of POPI, a Data Subject may either be a natural or a juristic person. Medpace processes personal information relating to the following categories of data subjects and information:

- Participants in a clinical trial;
- Personnel / employees of study sites;
- Medpace employees, consultants, and contractors; and
- Other third parties with whom Medpace conducts business including vendors, sponsors, ethics committee, third-party consultants, and regulators.

XII. Categories of Information

In respect of natural persons may include: name, identifying number (identity or passport number), date of birth, citizenship, age, gender, race, marital status, language, telephone number(s), email address(es), physical and postal addresses, income tax number, banking information, health information, genetic information, biometric information, employment history, background checks, fingerprints, CVs, education history, remuneration and benefit information, details related to employee performance and disciplinary procedures.

All information regarding clinical trial participants is coded so that the Personal Information collected cannot be linked by Medpace to an identified or identifiable person.

With respect of juristic persons, information collected may include name, registration number, tax information, contact details, physical and postal addresses, FICA documentation, payment details (including bank accounts), invoices and contractual agreements.

XIII. Planned transborder flows of Personal Information [Section 51(1) (c)(iv)]

POPIA provides that Personal Information may only be transferred out of the Republic of South Africa if:

- The Recipient country can offer such data an "adequate level" of protection (its data privacy laws must be substantially similar to the Conditions for Lawful Processing as contained in POPI); or
- The Data Subject consents to the transfer of their Personal Information; or
- The transfer is necessary for the performance of a contractual obligation between the Data Subject and the Responsible Party; or
- The transfer is necessary for the performance of a contractual obligation between the Responsible Party and a third party, in the interests of the Data Subject; or
- The transfer is for the benefit of the Data Subject, and it is not reasonably practicable to obtain the consent of the Data Subject, and if it were, the Data Subject, would in all likelihood provide such consent.

Medpace may transfer personal information to third parties or other Affiliates of Medpace, who are situated in a foreign country and such transfers are subject to the relevant provisions of the POPI Act.
In addition, Personal Information may be transmitted transborder to Medpace suppliers in other countries, and Personal Information may be stored in data servers hosted outside South Africa. Medpace will endeavor to ensure that its business partners, Affiliates, and suppliers will make all reasonable efforts to secure Personal Information under its control.

XIV. Information security measures [Section 51(1) (c)(v)]

Medpace strives to take appropriate, reasonable technical and organizational measures to secure the integrity and confidentiality of personal information in its possession or under its control. The details given below are to be interpreted as examples of how to achieve an adequate data protection level for each objective. Medpace may use alternative measures and adapt to technological security development, as needed, provided that the objectives are achieved.

- Access Control: suitable measures to prevent unauthorized persons from gaining access to the data processing equipment where the data are processed.

- Data Media Control: suitable measures to prevent the unauthorized manipulation of media, including reading, copying, alteration or removal of the personal data.

- Data Memory Control: suitable measures to prevent unauthorized input into data memory and the unauthorized reading, alteration or deletion of stored data.

- User Control: suitable measures to prevent its data processing systems from being used by unauthorized persons by means of data transmission equipment.

- Access Control to Data: the persons entitled to use data processing system are only able to access the data within the scope and to the extent covered by their respective access permissions.

- Transmission Control: verification and tracing of the locations / destinations to which the personal information is transferred

- Transport Control: suitable measures to prevent Personal Information from being read, copied, altered or deleted by unauthorized persons during the transmission thereof or during the transport of the data media.

XV. Objection to processing of personal information [POPIA Regulation 2]

A data subject may at any time object to the processing of his / her / its Personal Information (as contemplated in Section 11(3)(a) of the POPI Act) by contacting the Information Officer in the manner described in this POPI Manual, subject to exceptions contained in the Acts.

XVI. Requests for correction or deletion of Personal Information [POPIA Regulation 3]

A data subject may at any time request the correction or deletion his / her / its Personal Information (as contemplated in Section 11(3)(a) of the POPI Act) by contacting the Information Officer in the manner described in this POPI Manual, subject to exceptions contained in the Acts. Please note that Personal Information collected from clinical trial participants may not be corrected or deleted. Clinical trial participants who wish to withdraw their consent to participate in a clinical trial should contact the study doctor and/or the study site at which they are participating to obtain additional information about withdrawing from the study.