



Neimeth International Pharmaceuticals PLC Personal Data Breach Management Procedure



Contents

1. INTRODUCTION/SCOPE.....	3
2. AIMS AND OBJECTIVES	3
3. PERFORMANCE AND MONITORING OF RESPONSIBILITIES	3
4. DATA BREACH MANAGEMENT PROCESS.....	4
5. DISCIPLINARY.....	6
6. RELATED POLICIES AND PROCEDURES	6
7. CHANGES TO THE POLICY	6
8. CONTACT FOR ANY QUERIES.....	6
APPENDIX 1.....	7
APPENDIX 2.....	8
APPENDIX 3.....	10



1. INTRODUCTION/SCOPE

Neimeth International Pharmaceuticals PLC (“the Company”) is committed to ensuring that the personal data it collects and processes is stored securely and protected from un-authorized access. This Personal Data Breach Management Policy (Policy) sets out the procedure to be adopted for dealing with incidents leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

This Policy applies to all employees, that collect, access, use, store or process personal data on behalf of Neimeth International Pharmaceuticals PLC.

2. AIMS AND OBJECTIVES

2.1 This Policy aims at raising awareness of what constitute Personal Data Breach cases (Data Breach) and to ensure that Data Breaches are easily identified and appropriate measures are taken to contain such incidents.

2.2 When a potential breach incident is reported, the Company will investigate to determine if an actual breach has occurred and take steps to manage and investigate the breach as follows:

- a) Validate the personal Data Breach and ensure that Data Breaches are appropriately identified and managed in accordance with the law and best practice.
- b) Ensure that a proper and impartial investigation is initiated, conducted, documented and concluded.
- c) Identify remediation requirements and track resolution.
- d) Ensure the impact of the incident is understood, and action is taken to prevent further damage.
- e) Report findings to the executive management.
- f) Ensure that impacted Data Subjects are properly notified, if necessary.
- g) Ensure incidents are reviewed and appropriate control mechanisms are put in place to prevent a reoccurrence.

3. PERFORMANCE AND MONITORING OF RESPONSIBILITIES

3.1 All employees are responsible for reporting actual, suspected, threatened or potential personal data breach incidents or information security incidents and for assisting with investigations as required, particularly if urgent actions must be taken to prevent further damage.

3.2 All suspected Data Breach incidents must be reported immediately it is identified to the Data Protection Officer (“DPO”) to ensure that:

- a) any reporting duties under the Nigeria Data Protection Regulation, 2019 (NDPR) and other applicable laws can be complied with;
- b) any affected Data Subject can be informed; and
- c) any stakeholder communication can be managed.

3.3 Examples of Data Breaches include but are not limited to the following:

- a) improper transmission of personal data across borders;
- b) loss or theft of data or equipment on which data is stored;



- c) accidentally sharing data with someone who does not have a right to know this information;
- d) inappropriate access controls allowing unauthorized use;
- e) equipment failure which results in a data breach;
- f) human error resulting in data being shared with someone who does not have a right to know;
- g) hacking attack; and
- h) any other incident of data breach.

3.4 The DPO and the Neimeth International Pharmaceuticals PLC Data Breach Response Team (**See Appendix 1**) shall be responsible for the coordination and handling of any data breach incident in a timely and efficient manner.

3.5 Data security breaches should be reported promptly to the DPO as the primary point of contact by completing the Data Breach Report Form. (**See Appendix 2**).

3.6 Suspected Data Breaches that are discovered to be false alarms or “near miss” events and do not cause immediate harm to individuals or the organization will not result in formal action. However, such suspected Data Breaches should still be reported and logged, as analysis of these will allow lessons to be learnt and enable continual improvement.

4. **DATA BREACH MANAGEMENT PROCESS**

4.1 Once a Data Breach has been reported, the following procedure and relevant response plan must be followed to ensure appropriate management of the Data Breach incident:

4.1.1 **Containment and Recovery**

- a) Once it has been established that a Data Breach has occurred, Neimeth International Pharmaceuticals PLC will take immediate and appropriate action to limit the breach and damages as much as possible through restoring of lost/damaged data, interviewing the key personnel involved in the Data Breach and their line managers and collecting as much information as possible.
- b) An investigation would be conducted and a preliminary update should be provided to management within 48 hours of the occurrence of the breach to allow Neimeth International Pharmaceuticals PLC evaluate the Data Breach and make the required notification to the National Information Technology Development Agency (NITDA) within the stipulated timelines (**See Section 4.1.3 below**). A full-scale investigation should be completed within 5 working days of the Data Breach and a detailed report should be presented to the Management even when the case cannot be concluded within this timeframe.
- c) Further reports should be presented to Management at least every 10 working days until the case is concluded.



4.1.2 Risk Assessment

Neimeth International Pharmaceuticals PLC will carry out a risk assessment to consider the potential adverse consequences of the Data Breach to Data Subjects and to Neimeth International Pharmaceuticals PLC. This will include an evaluation of the causes of the incident and the effectiveness of Neimeth International Pharmaceuticals PLC's response, as well as identifying lessons to be learned. The risk assessment will help inform decisions about remedial actions and notification.

4.1.3 Notification

In the event of any data breach incident, Neimeth International Pharmaceuticals PLC shall notify NITDA within **72 hours** of the knowledge of the breach, in line with the provisions of the NDPR. The report would detail the number of data likely to be affected, cause of the breach and remedial actions being taken by Neimeth International Pharmaceuticals PLC to remedy the breach.

In particular, the notification to NITDA will include the following:

- a. A description of the circumstances of the loss or unauthorized access or disclosure;
- b. The date or time period during which the loss or unauthorized access or disclosure occurred or continued;
- c. A description of the personal information involved in the loss or unauthorized access or disclosure;
- d. An assessment of the risk of harm to individuals as a result of the loss or unauthorized access or disclosure;
- e. An estimate of the number of individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure;
- f. A description of any steps Neimeth International Pharmaceuticals PLC has taken to reduce the risk of harm to individuals;
- g. A description of any steps Neimeth International Pharmaceuticals PLC has taken to notify individuals of the loss or unauthorized access or disclosure, and
- h. The name and contact information for a person who can answer (such as the DPO), on behalf of Neimeth International Pharmaceuticals PLC's NITDA's questions about the loss of unauthorized access or disclosure.

In addition to any notification to NITDA and based on the evaluation of risks and consequences, the DPO shall determine whether it is necessary to notify the Data Subject(s) about the Data Breach incident. The report to the affected Data Subject shall be in the prescribed Data Breach Notification Form (**See Appendix 3**)



Before any external report is made (whether to NITDA or Data Subject), relevant stakeholders and in particular the Neimeth International Pharmaceuticals PLC's Data Breach Management Team need to be engaged in the drafting of the relevant notification and to also ensure that Neimeth International Pharmaceuticals PLC can adequately deal with any external inquiries that may be directed at the Company as a result of the breach.

4.1.4 Evaluation and Response

Neimeth International Pharmaceuticals PLC will review the causes of the incident and the effectiveness of Neimeth International Pharmaceuticals PLC's response, to ensure that the steps taken during the incident are appropriate and identify areas that may need to be improved.

- 4.2 The DPO shall compile the record of all personal Data Breaches and will report the incident in a Data Breach Incident Register/Log in order to identify lessons to be learned, patterns of incidents and evidence of weakness and exposures that need to be addressed.

5. DISCIPLINARY ACTIONS

Violation of this Policy may result in disciplinary actions. This may include termination of employment and/or dismissal for employees or other appropriate sanctions.

6. RELATED POLICIES AND PROCEDURES

6.1 This Policy shall be read in conjunction with all the data privacy and protection policies of Neimeth International Pharmaceuticals PLC.

6.2 All employees should ensure compliance with the above policies and procedures.

7. CHANGES TO THE POLICY

Neimeth International Pharmaceuticals PLC reserves the right to change, amend or alter this Policy at any point in time. If we amend this Policy, we will provide you with the updated version.

8. CONTACT FOR ANY QUERIES

Neimeth International Pharmaceuticals PLC has appointed a DPO responsible for overseeing Neimeth International Pharmaceuticals PLC's data protection strategy and its implementation to ensure compliance with NDPR requirements.

The DPO should be contacted if you have any queries or clarifications regarding the operation of this Policy. The contact details are set out below:

- Data Protection Officer:
- Location: Legal Unit, Neimeth International Pharmaceuticals Plc .
- Phone: 08140246475
- Email: dpo@neimethplc.com.ng



APPENDIX 1

Neimeth International Pharmaceuticals PLC's Data Breach Management Response Team

The Data Breach Management Response Team consists of the following:

S/N	Department/Unit	Designation	Assigned Tasks
1	Information and Communications Technology (ICT)	Head IT	Evaluate the security breach and contain same.
2.	Legal	Head Legal	Evaluate the legal and regulatory impacts of the breach and remedial steps
3.	Human Resources	Head HR	Evaluate the risk and provide relevant support and advice.
4	Customer Service	Head Customer Care	Internal and External Communications, including communication to Data Subject and the Regulator.
5.	Data Protection Officer	DPO	Evaluate the risk and coordinate the activities of relevant stakeholders



APPENDIX 2

Personal Data Breach Report Form

If you discover any Personal Data Breach, please notify your line manager and the Data Protection Officer of Neimeth International Pharmaceuticals PLC immediately. Please complete this form, return it to the Data Protection Officer by email to dpo@neimethplc.com.ng

Your initial response should be provided within 12 hours of the Data Breach.

NOTIFICATION OF DATA SECURITY BREACH	TO BE COMPLETED BY ANY PERSON REPORTING BREACH OF PERSONAL DATA
Date and time of detection:	
Date(s) and time of the Data Breach:	
Place of Data Breach:	
Type of Breach	
Data Subject(s) affected	
Name of person reporting incident:	
Contact details of person reporting incident (email address, telephone number, UCD address):	
Brief description of incident or details of the information affected:	
Number of Data Subjects affected, if known:	
Has any personal data been placed at risk? If, so please provide details	
Brief description of any action taken at the time of discovery:	



NOTIFICATION OF DATA SECURITY BREACH	TO BE COMPLETED BY ANY PERSON REPORTING BREACH OF PERSONAL DATA
Was the incident reported and to who?	
<i>For Information of Data Protection Officer</i>	
Report received from:	
Date:	
Action:	
Date:	



APPENDIX 3

[This Data Breach Notification is to be sent to Data Subject (s) whose personal data has been breached and where there is a high risk of exposure]

Dear XXXX,

Data Breach Notification

We write to notify you about a data security incident that occurred within Neimeth International Pharmaceuticals PLC involving your personal data. The security breach occurred on XXXXX as a result of *(please provide details of the personal data breach)*. We discovered that the data accessed, include your personal data such asemail address, phone number and residential address.

We have engaged digital security experts to conduct an examination of our data system and put in measures to mitigate any likely risk that may arise as a result of the breach and to prevent future occurrence of such security incident. We will keep you informed in the event of any discovery of a potential threat that you might be exposed to as a result of the security breach.

Once again, we reassure you that the security and privacy of your personal data which you have with Neimeth International Pharmaceuticals PLC is of utmost importance to us. Neimeth International Pharmaceuticals PLC remains committed to the protection of your personal data. Please contact our Data Protection Officer via for further enquiries or information on how we protect your personal data.

Yours faithfully,

.....
Neimeth International Pharmaceuticals PLC
Data Protection Officer