PROCEDURE TO FOLLOW WHEN A BREACH OR INCIDENT OCCURRED

1. Introduction

As a Society that holds personal information of its members/data subjects, BP Medical Aid Society must ensure appropriate measures are in place to protect against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

In the event of a data breach or an information security incident, it is therefore vital that appropriate actions are taken to promptly report the breach to the Information Officer who will manage the incident and minimise associated risks.

2. What is a data breach?

A data breach or incident occurs when the conditions for lawful processing of personal information, as described in the Protection of Personal Information Act (POPIA), are breached. These conditions include, but is not limited to accountability, processing limitations, purpose specifications, further processing limitation, information quality, openness, security safeguards and data subject participation.

3. Purpose

This procedure is designed to set out the process that should be followed to ensure a consistent and effective approach is in place for managing a data breach across the Society and the operators and to ensure that:

- Data breach events are detected, reported, and monitored consistently.
- Incidents are assessed and responded to appropriately.
- Action is taken to reduce the impact of a breach.
- Relevant breaches are reported to the Information Officer immediately.
- Improvements are made to prevent recurrence.
- Lessons learnt are communicated to all staff and operators.

4. Responsibilities

4.1 Information Officer

The Information Officer of the Society has responsibility to the Trustees for ensuring that any privacy risks are managed.

4.2 All Staff

All users of information assets across the Society should familiarise themselves with this procedure, be aware of privacy risks and be vigilant to ensure breaches are identified, reported and managed in a timely manner.

5. Procedures

The data breach reporting process is explained below.

5.1 Identify a data breach/suspected data breach

A data breach can happen for several reasons, for example:

- Loss or theft of data or equipment on which data is stored, or through which it can be accessed.
- Loss or theft of paper files.
- Hacking attack.
- Inappropriate access controls allowing unauthorised/unnecessary access to data.
- Equipment failure.
- Human error.
- Unforeseen circumstances such as a fire or flood.

5.2 Reporting an Incident

It is vital that as soon as a data breach is identified or suspected it is immediately reported to the Information Officer. In order to improve our understanding of the risks to data and address them before breaches occur, individuals are encouraged to report 'near misses' (i.e. incidents which have almost resulted in a data breach except for an intervention or 'luck'). Near misses should be reported using the same form and process as an actual breach highlighting clearly that the incident is a near miss.

As much information as is immediately available should be collated and the data breach identified. The Information Officer will analyse the breach, update the data breach log, and ascertain whether any immediate corrective/containment/escalation actions are required.

5.3 Investigating an Incident

Depending on the type and severity of the incident the Information Officer will assess whether a full investigation into the breach is required. Where required, the Information Officer will appoint an appropriate investigation team who will complete a full breach report. The investigation will:

a) Establish the nature of the incident, the type and volume of data involved and the identity of the data subjects.
b) Consider the extent of a breach and the sensitivity of the data involved.
c) Perform a risk assessment.
d) Identify actions the Society needs to take to contain the breach and recover information.
e) Assess the ongoing risk and actions required to prevent a recurrence of the incident.

5.4 Reporting a Breach to the Data Subject/Member

The Information Officer will evaluate whether the breach is '*likely to result in a high risk to the rights and freedoms'* of the data subject. If this is determined to be the case the incident will also be reportable to the data subjects without undue delay. Any such report will be coordinated by the Information Officer, with assistance from Society Management and the applicable operator.