DATA PROTECTION POLICY

Table of Contents

1. Introduction and purpose

1.1 Mitera Health HMO is required to collect and maintain certain personal data about individuals for the purpose of satisfying our statutory, operational and regulatory obligations.

1.2 Data Protection law[1] places requirements on the Mitera Health HMO which includes Team members (including contractors), Board members, Health Care Provider members. It is the responsibility of all Mitera Health HMO, her Contractors and Health Care Provider members to protect the personal data of data subjects by following this policy and the associated guidance.

1.3 Mitera Health HMO is a Data Controller, as defined in the Nigeria Data Protection Regulation (NDPR), and must ensure that all of the data protection requirements are implemented.

1.4 The purpose of this policy is to outline the key principles of data protection law and set out how MITERA HEALTH HMO meets its legal obligations to ensure that all data is held and processed in compliance with data protection law. All employees and contractors of the Mitera Health HMO must read this policy.

2. The Data Protection Law

2.1 Data Protection law provides a framework of rights and duties which is designed to safeguard personal data. The law balances the needs of organisations to collect and use personal data for clear, legitimate purposes against the individuals rights to privacy. Wherever data is held, whether it is papers, complaints records, emails or any other records), the rights of the individual to privacy and access apply.

2.2 The law applies to paper and electronic records and audio and visual recordings, and does not differentiate between these different types of records. If an individual is identifiable then the records contain personal data and therefore the data protection obligations apply.

2.3 Compliance with data protection law is regulated by the Nigeria Data Protection Commission who has various powers, including issue of an enforcement notice (breach of which is a criminal offence) and the ability to fine organizations for failing to comply. If an individual unlawfully obtains or discloses personal data they could be committing a criminal offence.

2.4 There are also wider implications for failing to comply with data protection law - disclosure of personal data can cause real harm, damage or distress to individuals; there is a risk of compensation claims by those affected; the Nigeria Data protection commission can publicize security breaches leading to

[1] Data Protection law includes the Nigerian General Data Protection Regulation, the Law Enforcement Directive, the Privacy and Electronic Communications Regulations, the current Data Protection Act and the Data Protection bill

reputational damage; and stakeholders may lose trust in the way MITERA HEALTH HMO manages personal data. We are all individually responsible for protecting personal data.

3. Data Protection Principles

Data Protection law sets out six principles by which personal data must be processed. Along with the 6 Principles there is an overarching Accountability requirement. MITERA HEALTH HMO must ensure that personal data is:

1. processed fairly, lawfully and transparently
2. collected for explicit and lawful purposes and processed in a manner compatible with those purposes (purpose limitation)
3. adequate, relevant and not more than necessary for those purposes (dat minimisation)
4. accurate and up to date, inaccuracies should be changed without delay
5. kept only as long as is necessary
6. processed securely and protected against unauthorised or unlawful processing, loss or destruction

3.1 Principle 1 - Personal data shall be processed fairly, lawfully and in a transparent manner in relation to the data subject

In practice, Principle 1 means that the Mitera Health HMO must:

- have legitimate grounds for collecting and using personal data;
- not use personal data in ways that have unjustified adverse effects on individuals;
- be transparent about how we intend to use personal data, and give individuals appropriate fair processing notices (privacy notices) when collecting their personal data;
- handle personal data only in ways individuals would reasonably expect;
- make sure we do not do anything unlawful with the data.

3.1.1 Conditions for processing

Processing means collecting, recording, using, disclosing, transferring, retaining or disposing of personal data or carrying out any operation or set of operations on the personal data, including –

- organisation, adaptation or alteration of the data
- retrieval, consultation or use of the data
- disclosure of the data by transmission, dissemination or otherwise making available
- alignment, combination, blocking, erasure or destruction of the data

If any aspect of processing is unfair, there will be a breach of this principle.

Before we can process any individual's personal data we must ensure that conditions for processing are met. The conditions for processing are set out in the Schedules of data protection law. When processing special category (sensitive) personal data, we must be able to demonstrate

that there are two conditions that apply under the appropriate two Schedules detailing conditions for processing.

3.1.2 Fair processing notices/Privacy Notices

When personal data is collected about individuals, they should be told exactly how that data is to be used. This is called a fair processing notice or privacy notice. It is important that such notices are concise, transparent, intelligible and easily accessible. It must be written in clear and plain language, especially if the notice is for a child. So it's important that any privacy notices specifically for children is clear and in a language that they will understand. The notice should tell them:

- Who MITERA HEALTH HMO is, including name and contact details;
- Contact information of the Data Protection Officer (DPO)[2];
- why we need their data, it must be fair and lawful;
- what purpose we will use it for (and it will not be used for any purpose incompatible with the original purpose);
- the categories[3] of personal data obtains and the source of the data (if the data hasn't been collected directly from the individual);
- if the collection of data is consensual, contractual or legal obligation and, if it is consent based, how to withdraw consent;
- who we will share it with (and what they will use the data for);
- about their rights under data protection law, including the right to access, amend, restrict and erase the information we hold about them;
- the details of the existence of automated decision making, including profiling (if applicable);
- how they can make a complaint to the regulator
- how we will ensure that the data is kept secure, accurate and up to date
- how long we will keep the data[4] and that we will dispose of data securely
- if the information is to be transferred out of the Nigerian Economic Area (NEA)

If the data is collected by another organisation, it is important to provide the individuals with the notice when we receive the data. A record of the privacy notice should be held for as long as the data itself is held.

If you think someone would not know about the use of their data, or would find it objectionable in any way that causes detriment to an individual then it is necessary to tell them about it. This is 'actively communicating' a privacy notice and means that we will tell an individual about the collection and processing of their personal data. This is different to having a privacy notice available for individuals to access if they want to find out more about how we handle personal information. We will also actively communicate a privacy notice when collecting sensitive personal data.

[2] The DPO in MITERA HEALTH HMO is the Information Governance Lead (IGL)
[3] See MITERA HEALTH HMO Privacy Notices for further information
[4] Please refer to MITERA HEALTH HMO' *Retention and Disposal Schedule* for guidance.

MITERA HEALTH HMO has a privacy notice on our corporate website for members of the public. There is one specifically for volunteers and staff. If there is a change to how we process personal data, please speak to the IG Team for advice to ensure that individuals are fully informed of how we use their data.

When making fair processing notices available, the same medium will be used to deliver the notice as is used to collect the information. For example, if the information is being collected through a website, the notice will also be available on the website.

3.1.3 Disclosure of personal information to third parties

Information about identifiable individuals should only be disclosed on a need to know basis. The validity of all requests for disclosure of personal data without consent from the data subject must be checked. The identity of those requesting data and their legal right to request or demand information must be validated. The reasons for any disclosure made without consent must be documented.

Police officers or others requesting information for the purposes of a criminal investigation should be asked to put their request in writing. The request should include:

- what information is required
- why it is needed
- how the investigation will be prejudiced without it

This requirement can be set aside where the request is made in an emergency (i.e. a person is in immediate and imminent risk of serious harm).

Decisions related to the disclosure of information to third parties must be taken at an appropriately senior level within MITERA HEALTH HMO. If an AST member, panel member or Clerk, receives an information request they must alert the MITERA HEALTH HMO IT Security Team.

Any member of MITERA HEALTH HMO staff or contractor, who is required to send personal identifiable data in any format to countries outside the Nigerian Economic Area, must discuss this with MITERA HEALTH HMO as the levels of protection for the information may not be as comprehensive as those in Nigeria.

3.1.4 Information Sharing

MITERA HEALTH HMO will produce Data Processing Contracts, Information Sharing Protocols and Data Access Agreements where necessary in order to ensure the secure and lawful transfer of personal data between parties.

3.1.5 Data Protection Impact Assessments (DPIAs)

MITERA HEALTH HMO will conduct DPIAs prior to initiating a project which will involve the collection/use of personal data, in order to assess the privacy risks to individuals. There are guidance and templates available

for the MITERA HEALTH HMO National Team to complete these impact assessments and the IG Team will provide assistance and guidance where necessary.

3.2 Principle 2 - Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

In practice, Principle 2 means that the Mitera Health HMO must:

- be clear from the outset about why we are collecting personal data and what we intend to do with it
- ensure that the reasons for processing the personal data are clear and specified – including in privacy notices
- annual notification fee to the regulator
- ensure that if we wish to use or disclose the personal data for any purpose that is additional to the originally specified purpose, the new use or disclosure is fair and lawful and is compatible with the original purpose

3.2.1 Notification

MITERA HEALTH HMO must provide an annual notification to the Nigeria Data Protection Commission. The Nigeria Data Protection Commission will require the name and address of the controller, staff numbers, financial turnover and contact information of the Data Protection Officer (DPO, and if applicable the individual completing the registration.

3.2.2 Incompatible re-use of information

MITERA HEALTH HMO will be open and transparent about the way in which we process personal data. Personal data must not be re-used for any purpose that is incompatible with the original purpose for which it was collected.

3.2.3 CCTV

CCTV cameras collect personal data in the form of images, as such if CCTV footage is to be collected individuals should be appropriately notified of its use through fair processing notices (see section 3.1.2)

CCTV cameras are in operation at the entrances and in the car park. These cameras are owned by Mitera Health HMO and the images are monitored by the Mitera Health IT Security Team. The images are held in line with Mitera Health HMO policies and procedures.

3.3 Principle 3 - Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (Data Minimisation)

In practice, Principle 3 means that the Mitera Health HMO must:

- only hold personal data about an individual that is sufficient for the purpose we are holding it for in relation to that individual
- ensure that we hold enough data that is adequate for the purposes we are holding it for
- not hold more data than we need for that purpose (data minimisation)

Personal data should not be held on the off chance that it may be useful in the future. However, it is permissible to hold personal data for a foreseeable event that may never occur.

Where special category (sensitive) personal data is concerned, it is particularly important to make sure that we collect or retain only the minimum amount of data we need.

3.4 Principle 4 - Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay

In practice, Principle 4 means that the Mitera Health HMO must:

- take reasonable steps to ensure the accuracy of any personal data we obtain
- ensure that the source of any personal data is clear
- carefully consider any challenges to the accuracy of data held
- consider whether it is necessary to update the data

The law recognises that it may not be practical to double-check the accuracy of every item of personal data we process. The law makes special provision about the accuracy of information that individuals provide about themselves, or that is obtained from third parties.

Each Information Asset Owner (IAO) will undertake a regular audit of their information asset to ensure that it is accurate and up to date.

3.4.1 Health Care Providers member contact details

It is the responsibility of each panel and Health Care Providers member to ensure that their name and contact details are accurate and up to date. Health Care Providers members may update their own record or notify the MITERA HEALTH HMO IT Security Team of any changes, and a member staff will update their record on their behalf.

MITERA HEALTH HMO and Health Care Providers are responsible for ensuring that the remaining record is accurate and up to date.

3.5 Principle 5 - Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes

In practice, Principle 5 means that the Mitera Health HMO must:

- review the length of time we keep personal data
- consider the purpose or purposes we hold the data for in deciding whether (and for how long) to retain it
- securely dispose of data that is no longer needed for this purpose or these purposes
- update or securely dispose of data if it goes out of date

Mitera Health HMO members must ensure that they are aware of, and comply with, MITERA HEALTH HMO' *Retention and Disposal Schedule*.

3.6 Principle 6 - Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

In practice the Principle 6 means that MITERA HEALTH HMO must have appropriate security measures to prevent the personal data held being accidentally or deliberately compromised. In particular, MITERA HEALTH HMO must:

- design and organise our security to fit the nature of the personal data we hold and the harm that may result from a security breach
- be clear about who is responsible for ensuring information security
- make sure we have the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff
- be ready to respond to any breach of security swiftly and effectively

3.6.1 Keeping personal information safe and secure

Organisational security:

- MITERA HEALTH HMO has an Information Governance Policy Framework in place with four overarching policies: **Information Security**, **Data Protection, Acceptable Use** and **Records Management.**
- MITERA HEALTH HMO has a suite of policies, procedures and guidance which support the above policies and govern the processing of personal data.
- MITERA HEALTH HMO highlights information risks on its strategic risk register which is considered by the Audit and Risk Management Committee and MITERA HEALTH HMO Board on a regular basis.
- Only authorised people can access, alter, disclose or destroy personal data and those people only act within the scope of their authority.
- Mitera Health HMO members must undergo mandatory data protection training and complete refresher training on a regular basis.
- Mitera Health HMO members must read, understand and comply with this policy and accompanying policies, procedures and guidance for managing information.

- Personal information must not be disclosed, accidentally or otherwise to any unauthorised third party.
- MITERA HEALTH HMO has data processing contracts in place with data processors across the country and carries out audits of these data processors, in line with Principle 6.

Physical security:

MITERA HEALTH HMO Staff and Board members:

- Access to the MITERA HEALTH HMO office is governed by Mitera Health HMO's *Information Access Control Security Policy*.
- Visitors must be signed in and out of the premises.
- Confidential paper waste must be disposed of in the office shredding bin and a member of MITERA HEALTH HMO staff must witness paperwork being shredded.
- MITERA HEALTH HMO operates a clear desk policy.
- Personal data in the form of manual records must be kept in a locked filing cabinet, drawer or other secure area.

Staff, contractors and Health Care Providers Staff members:

- Confidential paper waste must be disposed of using a cross-cut shredder or by handing to the Clerks for secure destruction.
- Staff, contractors and Health Care Provider must ensure when handling personal data at home that it is kept out of sight and in a safe place and that no other members of the household can access the personal data.
- Staff, contractors and Health Care Provider members must ensure that personal data is placed within a zipped/locked bag when travelling to a hearing/meeting.
- When travelling to a hearing/meeting, members must lock the zipped/locked bag in the boot of the car or another secure area (e.g. glove box).
- Personal data must not be accessed/read while on public transport or when in public places.
- Personal data must not be left unattended at any time – this includes information on a computer screen and information on paper documents.
- Clerks must keep information relating to the System separate from local authority information on electronic systems

IT Security:

- IT equipment must be disposed of in a secure manner in line with MITERA HEALTH HMO guidance. To arrange disposal of ICT equipment please contact securtiy@miterahealth.com.ng
- Access to special category (sensitive) personal data is protected by placing additional controls on access.
- Personal data in the form of computerised records will be kept on a secure IT system which is either password protected, encrypted or has additional device security.
- Personal data must not be kept on unsecure portable data storage devices.
- Laptops must be kept in a secure location at all times
- MITERA HEALTH HMO staff must lock their computer screens (ctrl-alt-del) when away from their desks.
- MITERA HEALTH HMO staff must lock their laptops to their docking station when in the office.

- Mobile phones must be locked with a PIN/password.

In addition to the measures highlighted above, MITERA HEALTH HMO has an Information Governance Policy Framework in place which identifies each of the IG policies and procedures in existence and to whom it applies to in the Mitera Health HMO. Guidance on managing information appropriately and in line with our statutory obligations can be found in the relevant policies and procedures. There are four overarching policies, which include, this policy, the Information Security Policy, the Records Management Policy and the Acceptable Use Policy.

3.6.2 Data Processors

Where MITERA HEALTH HMO uses a third party to process personal data on its behalf, the contractor must sign a Data Processing Contract which ensures that they are taking adequate steps to comply with Principle 6 (and all other data protection requirements) on MITERA HEALTH HMO' behalf. Data Processors have legal obligations under data protection law, as well as the explicit instructions contained within the data processing contract. Data Processors must report any security incident to MITERA HEALTH HMO immediately. MITERA HEALTH HMO retains legal responsibility as data controller and it's important that the contracts are detailed and clear on what the data processors can and can't do. Therefore it's important that those managing contracts must ensure that all security procedures necessary are specified in the contract, and it is subsequently monitored to ensure that they are in place. This includes carrying out audits regularly to ensure that the contract obligations are being met.

4. Data Subjects Rights

As well as the 6 Principles under data protection law, the individuals (i.e. data subjects) have additional rights under the legislative framework.

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure (commonly known as the right to be forgotten (RTBF)
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

4.1.1 The Right to be Informed

This links with Principle 1 and the transparency requirement to actively communicate privacy notices to the individuals. As referenced earlier, individuals must be provided with a privacy notice detailing what we do with the personal data, how long it is kept, if it is shared who it is shared with, their rights under data protection law, including how to complain to the regulator etc.

4.1.2 Right of Access

Individuals have a right to request any of their personal data held by the Mitera Health HMO in whatever form. MITERA HEALTH HMO has a procedure to deal with requests for access to personal data (known as

Subject Access Requests - SARs). SARs will be handled by the MITERA HEALTH HMO National Team. If a SAR is received by a Health Care Provider, the MITERA HEALTH HMO IT Security Team should be notified within 2 working days.

SARs will be acknowledged by MITERA HEALTH HMO within 2 working days of receipt by MITERA HEALTH HMO (a request for proof of identification can be made at this time). The SAR will be responded to within one month of receipt of the request/identification. If any delays occur, MITERA HEALTH HMO will write to the data subject explaining the reason.

4.1.3 The Right to Rectification

This is the right for inaccurate personal data to be rectified or completed if it is incomplete. An individual can make a request for this in writing or verbally. As with the right of access, MITERA HEALTH HMO have one calendar month to respond. This links with principle 4 and the data controller's obligatiuons to keep personal data accurate and up to date.

4.1.4 The Right to Erasure (Right to be Forgotten)

This is a right which means individuals can request that the personal data held about them is erased. It is known commonly as the Right to be Forgotten (RTBF). Individuals can make the request to erase verbally or in writing. MITERA HEALTH HMO has one month to respond to a request. It's important to note that the right is not absolute and only applies in certain circumstances.

4.1.5 The Right to Restrict Processing

Individuals have the right to request the restriction or suppression of their personal data. AS with RTBF this is not an absolute right and only applies in certain circumstances. MITERA HEALTH HMO has a calendar month to respond to the request. It links closely to the Right to Rectification (see above). When processing is restricted, a data controller can store the data but not use it.

4.1.6. The Right to Data Portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move copy or transfer their data from one IT system to another in a safe and secure way without affecting its usability. Doing this enables individuals to take advantage of applications and services that can use this data to find them a better deal or help them understand their spending habits. As with the other rights this is not an absolute right, it only applies to information the individual has provided to the organisation.

4.1.7. The Right to Object

Individuals have the right to object to specific processing, based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling); direct marking (including profiling); and processing for purposes of scientific/historical research and statistics.

4.1.8 Rights in relation to automated decision making and profiling

The rights for individuals in relation to automated individual decision-making (making a decision solely by automated means without any human involvement); and profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of

an automated decision-making process. The rights mean that the privacy notice explains exactly how the decision making is made, how to request human intervent or challenge a decision.

5. Roles and responsibilities

5.1 MITERA HEALTH HMO Team and Board members

- The CISO has overall responsibility for data protection and information security. The CISO is responsible for ensuring that Mitera Health HMO members processing personal data receive the appropriate level of training to support the implementation of this policy. The CISO is also responsible for ensuring that all collection and processing of personal data complies with data protection law.

- The Chief Information Security Officer is designated as MITERA HEALTH HMO' Senior Information Risk Owner (SIRO). The SIRO is a senior member of staff responsible for information risk in the organisation. The SIRO is responsible for ensuring compliance with this policy and for assigning Information Asset Owners (IAOs) to information assets held by MITERA HEALTH HMO. Details of these IAOs can be found in MITERA HEALTH HMO' *Retention and Disposal Schedule*. The SIRO must also ensure that all Mitera Health HMO members, familiarize themselves with the content of this policy.

- The implementation of this policy is delegated to the Information Governance Lead (IGL) who is the designated Data Protection Officer (DPO) for MITERA HEALTH HMO. The IGL is responsible for identifying and publicising data protection responsibilities across the Mitera Health HMO.

- MITERA HEALTH HMO National Team and Board members are responsible for ensuring that they are familiar with and comply with this policy.

5.2 Mitera Health IT Security Team/DPO

- Mitera Health IT Security Team/DPO are responsible for raising awareness of data protection responsibilities and highlighting any data protection issues. In particular, they are expected to monitor compliance with this policy and other guidance issued by MITERA HEALTH HMO and report any suspected or known vulnerabilities and incidents in relation to the management of information, to MITERA HEALTH HMO. It is important that they report any incidents or vulnerabilities to the CISO **immediately** to ensure that where applicable MITERA HEALTH HMO can meet the required deadline of reporting a breach to the regulator within 72 hours. They are also expected to support MITERA HEALTH HMO in the investigation of any breaches of the policy or data protection law and to disseminate key IG messages at meetings.

5.3 Contractors

- All Contractors processing personal data are responsible for ensuring that they are familiar with and comply with this policy and other guidance issued by MITERA HEALTH HMO. Contractors are expected to assist in raising awareness of the importance of data protection and keeping information safe. Contractors expected to assist if a security incident occurs and should report any incidents to MITERA HEALTH HMO

IT Security Team immediately. Data protection training is provided to contractors.

5.4 Health Care Providers on Mitera Health Network

- **Health Care Providers** provide healthcare services to Mitera Health Enrollees. This service arrangement is governed by the Agreement between the Health Care Providers and MITERA HEALTH HMO.

- MITERA HEALTH HMO has put in place Data Processing Contracts (DPC) to govern the processing of personal data by Health Care Providers on behalf of MITERA HEALTH HMO. As data processors they have additional legal obligations, including reporting security incidents.

- Health Care Providers must report incidents to Mitera Health ICT Security Team when they become aware of an incident. This is important, as there is a duty to report serious breaches to the regulator within 72 hours of discovery.

6. Breaches of this policy

6.1 All personal data recorded in any format must be handled securely and appropriately in line with the DPA. MITERA HEALTH HMO staff and Board members, contractors and Health Care Provider members must not disclose information for any purpose outside their normal role.

6.2 Breaches of this policy by a member of MITERA HEALTH HMO staff will be considered as a disciplinary issue and will be investigated in line with the *Staff Code of Conduct*. Breaches of the policy by a Board member may lead to investigation by The Nigeria Data Protection Commission in line with the *Board member's Code of Conduct*. The Commission will investigate (or appoint a member of staff to investigate) any breaches of this policy by a Health Care Provider member. A breach of this policy by a Contractor or a member of their team will be handled in line with the terms of the Data Processing Contract.

7. Monitoring and Review

7.1 This policy will be reviewed every two years or as appropriate to take into account changes to legislation that may occur, and/or guidance from the Nigeria Data Protection Commission

Document Control

Title	Data Protection Policy
Author	Mitera Health IT Security Dept, October 2023
Approved by	MITERA HEALTH HMO Board
Date of approval	27th October 2013
Version number	3.0
Review frequency	Every two years
Next review date	October 2025

Appendix A: Definitions[5]

1.1 **Data** means information which:

a) is being processed by means of equipment operating automatically in response to instructions given for that purpose
b) is recorded with the intention that it should be processed by means of such equipment
c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system
d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68 or
e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d)

1.2 A **relevant filing system** is defined as: *"any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible."*

The NDPR's view is that this definition is intended to cover non-automated records that are structured in a way which allows ready access to information about individuals. As a broad rule, the NDPR considers that a relevant filing system exists where records relating to individuals (such as personnel records) are held in a sufficiently systematic, structured way as to allow ready access to specific information about those individuals.

1.3 **Personal data** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one of more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identify of that natural personal This can include application forms, complaints records, contact details etc.

1.4 **Special Categories of Personal Data** is information covering:

- the racial or ethnic origin of the data subject
- political opinions
- religious or philosophical beliefs
- membership of trade unions
- genetic data
- biometric data
- Data concerning health
- Data concerning a natural person's sex life or sexual orientation

5Further information about definitions is available from the NDPR website.

- the commission of any offence or criminal records

This type of data must be carefully handled. Additional security measures may be necessary to protect special category personal data.

1.5 The **Data Controller** is a person (usually an organisation) who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

1.6 The **Data Processor** means any person (other than an employee[6] of the data controller) who processes the data on behalf of the data controller.

1.7 The **Data Subject** is the living individual who is the subject of the personal data.

1.8 **Processing** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alternation, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

[6] Though MITERA HEALTH HMO does not consider volunteers as 'employees' in general, for the purposes of the Data Protection Act they are considered as such.