Health Data Protection Policy

The policy sets out the core principles and context considerations that provide the MSF framework for accountability, protection and security of patient and community data.

## Principles

Data protection principles should always be interpreted in a way that furthers the ultimate objective of humanitarian action, namely safeguarding the life, integrity and dignity of patients and communities.

### 1 Legitimate Grounds

MSF can only collect, use and transfer data...

- to provide health care
- to provide for a patient’s vital interest
- for communication & advocacy, with patient consent
- for health research, with patient consent

### 2 Purpose & Use Limitation

MSF shall be explicit and specific on the purpose for collecting, using and transferring data...

- use & share data only for these specific purposes
- secondary use for different purposes should respect safeguards in the policy
- put in place appropriate storage & archiving

### 3 Proportionality & Data Minimisation

MSF will only collect, use and transfer the minimum data necessary...

- data must be relevant to the specific legitimate ground
- access to data should be regulated & limited

### 4 Medical Confidentiality & Privacy

MSF shall only disclose data when the appropriate safeguards are in place...

- seek patient consent to disclose identifiable data to anyone not directly involved in his/her care
- respect ethical, legal & research rules when using data for research or advocacy

### 5 Do No Harm

MSF will systematically screen for risks ...

- assess the risk for collection, use & transfer of data
- explain & implement the necessary safeguards
- implement additional safeguards for highly sensitive data that can put patients, MSF or staff at risk

### 6 Transparency & Respect for Patients

MSF shall provide all relevant facts for patients to assess the consequences of their participation...

- information must be accessible & understandable
- wherever feasible, patients should be aware of their right to access, correct, delete their data & refuse to participate
- mitigate any issues when taking informed consent

### 7 Security

MSF shall assess the risks at each site where data is handled and implement security measures...

- protect data from improper disclosure, use & modifications
- store data safely, with access restricted to authorised personnel
- de-identify data when necessary & wherever possible

### 8 Accuracy

MSF will take all reasonable steps to ensure data collected is truthful, accurate and up-to-date...

- confirm accuracy & completeness of source data
- ensure reliability of patient data

---

**DATA TO PROTECT**

**Whose data?**

- patients in MSF supported facilities
- communities served by MSF
- participants in research supported by MSF

**Which data sources?**

- files linked to individuals or containing individuals’ personal data (patient records, images, video and audio)
- registers & tally sheets
- research data
- data used for advocacy
- GIS data

**What level of data identification?**

- identifiable
- indirectly identifiable (including de-identified data and data just with patient numbers)
- anonymous data that could cause harm to individuals, groups or MSF

**HIGHLY SENSITIVE DATA**

Especially data on ...

- violence-related injuries
- sexual violence
- termination of pregnancy
- patients tortured or in prisons
- data which reveals or implies racial or ethnic origin or political opinions
- disease where there is an obligation to abide by treatment

Can cause harm to ...

- patients
- potential patients
- their family
- groups or communities
- MSF & its staff

Can lead to ...

- harm
- stigmatisation
- discrimination
- violence

When principles conflict ...

- the best interest of the patient
- health ethics
- principle “do no harm” will guide MSF toward resolution

healthdataprotection@msf.org