MSF Health Data Protection Policy

April 2018

Adopted by MedOps, 13 March 2018*

Summary

MSF shall handle patient and community data responsibly, which includes respecting medical confidentiality, privacy, data protection and health ethics, laws, rules and practices. This policy sets out the core principles and context considerations that provide the framework for the protection and security of patient and community data at MSF. Data protection is an integral part of and supports humanitarian action. 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. MSF works in challenging humanitarian contexts and in situations of crisis. This means that protecting patient and community data is critically important, and pragmatic and flexible approaches need to be developed to support this.

MSF shall serve patients' and their communities' best interests first when it comes to any matter relating to their data. Unauthorised or inappropriate collection, use or transfer of patient or community data is a source of potential harm, especially when data is *highly sensitive*. All data shall be handled with consideration of possible risks and harm and MSF shall implement additional mitigating measures and precautions whenever data collection, use and transfer entails predictable consequential risks (such as stigmatization, discrimination or violence).

** MedOps is the international MSF platform composed of the Medical Directors and Operational Directors of each MSF Operating Centre.*

Index

Introduction

As a medical humanitarian organization MSF collects and uses the data of patients and communities to respond to their health and welfare needs. MSF also uses and transfers the data it collects for different purposes related to its humanitarian interventions, such as program monitoring and evaluation, audits, advocacy and research. **Confidentiality and medical ethics** are at the heart of MSF's medical practice and are central to maintaining trust and integrity in the patient-humanitarian worker relationship. Safeguarding patients' and communities' data is an essential aspect of protecting people's lives, their physical and mental integrity, and their dignity – which makes it a matter of fundamental importance for MSF. In all MSF's projects patients and their communities have a variable but important degree of vulnerability and unauthorized or inappropriate collection, use or transfer of their data is a source of **potential harm**. Responsible data management also preserves the **safety of MSF humanitarian action**, including that of its employees.

MSF needs a policy to ensure adequate data protection safeguards are in place to guarantee medical confidentiality and privacy and to minimize any risk of harm to patients, communities, MSF and its staff. At a time when data is ever more portable and accessible, MSF has a duty to enforce these data protection principles across all its projects and offices and ensure adherence by all those within or outside MSF involved in the handling of patient data. MSF shall serve patients' and their communities' best interests first when it comes to any matter relating to their data.

Special care and flexibility are required when applying data protection principles in MSF settings. Responsible management of patient data encompasses more than just good data protection; for example, it includes medical confidentiality, privacy and health ethics, laws, rules and practices. It also requires taking into account the specific scope and purpose of MSF humanitarian activities to provide for the urgent and basic needs of populations at risk, especially in emergency settings. **Data protection is an integral part of and supports humanitarian action**. 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 victims of humanitarian emergencies.

Objectives

This policy aims to:

- Introduce and define the core principles and context considerations as a framework for the protection and security of patient and community data at MSF.
- Act as a reference document, to sensitize, enhance responsible practice and support MSF in improving data protection through the promotion of responsible patient data management practices.
- Provide guidance for arbitrating decisions regarding patient data.
- Provide the basis for more detailed guidelines, protocols, tools and templates to implement these core principles.

Scope

This policy covers data and information on MSF patients, communities that MSF serves and target populations (together **"patient"** data) which is collected by or within MSF programs. Patient data is collected for a variety of reasons that are directly related to MSF's activities of health care, assistance, assessments and surveys, health promotion, disease prevention, public health, surveillance, program monitoring and evaluation, research and audits. The policy covers all data collected in MSF supported health facilities whether such data is

health, demographic, anthropologic, qualitative, historic or otherwise. It also covers data and information used for advocacy and communications which is collected in the activity of care or that is linked to MSF's assistance activities. This policy shall complement any wider data protection policy developed by MSF that encompasses minimum standards on all data collected, used and transferred by MSF.

The policy focusses on information and data that directly or indirectly identifies individuals (also known as personal data). MSF collects, uses and transfers identifiable data of patients, potential patients and their communities, contacts/ caregivers, general populations and research subjects. However, non-identifiable data can also cause harm. The policy also covers non-identifiable data, aggregate data sets, statistics, de-identified, anonymous and anonymised data that could cause harm to individuals, groups, communities, MSF or its staff should the data be misused. For example, in armed conflicts and other situations of violence, many threats are collective rather than individual – a village, a community as well as a specific group of men and women may all share the same threats. Likewise, information on a community with a high prevalence of disease in a context where individuals of that disease are stigmatized can cause harm if used in the wrong way.

This policy covers all operations performed on the data, including but not limited to its collection, recording, organization, adaptation/alteration, retrieval, consultation, use, access, analysis, collation, transmission, transfer, disclosure, sharing, storage, archiving, destruction or erasure (together **"collection, use and/or transfer"**).

Examples: below is a non-exhaustive list of files included in the scope of this policy (regardless of their format, whether paper, electronic or other):

- Files that include patient names (and all other data identifying a patient)
- Individual patient files and all other health files
- Audio and imaging materials, including pictures, videos and sound recordings
- Registers and tally sheets
- Data collected through a structured health information system
- Epidemiological data (including census and demographic data)
- Programmatic data up to the level of identifiable communities
- Public health surveillance
- Assessments
- Surveys (health, anthropological or social)
- Research data (medico-operational; prospective and retrospective; quantitative and qualitative; trials)
- GIS data
- Témoignage
- Biological samples and results of laboratory analyses
- Medical imaging, biometrics and all other techniques designed to identify individuals

"Highly Sensitive" data

All identifiable data concerning health, factors influencing health (for example, cultural and socio-economic details) and the history of individuals are sensitive and will be handled with care and professionalism.

In addition, any data (identifiable or not) that can be voluntarily or involuntarily misused against the interests of patients, potential patients, their family, groups or communities and/or MSF and its staff or put any of them at risk for political reasons, financial gain or any other reasons shall be treated as "highly sensitive" data. For example: data on violence related injuries; rape; termination of pregnancy; patients in prisons or detention centers; information on disease in a context where there is an obligation to abide by treatment; or data which reveals or implies racial or ethnic origin, political opinions, religious or philosophical beliefs, offences or sex life or preferences. Even some seemingly non-sensitive data can be highly sensitive in certain contexts (for example, details of cholera outbreaks).

MSF recognizes that all data should be handled with consideration of possible risks and harm.

Highly sensitive data should be subjected to the strictest application of this policy and its principles with additional mitigating measures. For example, if the handling of data entails predictable consequential risks (such as stigmatisation, discrimination or violence), in addition to any non-data protection measures (such as staff security), further data precautions based on the context should be taken to protect the individuals or communities by including more restricted access, higher security standards and stricter storage controls. As an illustration, programs dealing with sexual violence, health care for migrants as well as those involving audio-imaging materials or biometrics require higher levels of protection.

Furthermore, whenever MSF's collection, use or transfer of data is likely to result in a high risk to the rights and freedoms of individuals, groups, MSF or its staff, MSF should carry out an impact assessment (red flag system) which identifies, evaluates and addresses the risks arising from the proposed project and helps lead to measures that contribute to the avoidance or minimization of those risks. In some cases, it may be appropriate to refrain from the data operation in the first place.

Further detail on certain terms (for example, what is meant by "identifiable", "de-identified", "anonymous", "anonymised" and others) are included in Annex 1.

The Principles

I. Legitimate Grounds.

MSF must always have a legitimate ground on which to carry out any collection, use or transfer of data; it is the first step to be considered before embarking on a data operation. MSF can only collect, use and transfer data for the following legitimate grounds:

a) The data collection, use or transfer is necessary **to provide health care** to populations in distress, victims of natural or man-made disasters and armed conflict and people affected by epidemics and exclusion from healthcare i.e. based on MSF's mandate. This includes: preventive medicine, medical diagnostics, provision of health care and treatment, program management and evaluation, management of health care systems and services and medical/epidemiological surveillance.

b) The data collection, use or transfer is needed to provide assistance that is not direct health care but the **vital interests** of those assisted are at stake (for example: latrine construction in a cholera outbreak; food aid distribution; transfer of pharmacovigilance and serious adverse events data to regulatory authorities and research committees).

c) The collection, use or transfer of data is in support of MSF's assistance mandate, **based on informed consent** and for:
   - communication and advocacy to speak out on the situation and the fate of the population of concern to MSF; or
   - health research.

Which legitimate ground is used as the basis to collect, use or transfer data does not affect the fact that MSF shall seek consent for other ethical and/or legal reasons, for example, consent to surgery or irreversible medical procedures.

Responsible secondary use of data **for statistical, scientific and historical research purposes** (for example, use of data for research that was originally collected for health care) is permitted where it is in accordance with the terms of this policy (see *Specific Considerations* below on the secondary use of data for research).

II. Purpose and Use Limitation.

At the time of collecting data, MSF shall determine and explicitly set out all the specific purpose(s) for which the data being collected will be used, or for which it is contemplated that it could be used. This principle is in addition to the need for MSF to have a legitimate ground for the data operation and to comply with all other applicable legal and ethical issues (for example, when carrying out research, the need to have a protocol). MSF shall use and transfer data only for purposes compatible with the purpose(s) made explicit at collection and for responsible secondary use of data for scientific or historical research or statistics in accordance with this policy.

Storage Limits: Identifiable data will not be held for longer than necessary in relation to the purpose(s) it was collected or as legally required in the country of collection.

Safety, preservation and archiving of data (including handover)

Subject to conditions in-country, MSF shall store/ archive patient data safely and securely. Rules shall aim at ensuring: (a) continuity of patients' health care, notably in situations of displacement or for cases of chronic diseases; (b) preservation of evidence for patients that are victims of violence (for example if he/she decides years later to go to court and/ or claim compensation); (c) protection of victims of violence and medical confidentiality (in case of, for example, situations of conflict or fragile states, where the health authority may have no means to preserve the data and/ or represents a party to the conflict); (d) protection of MSF responsibility; and (e) ensuring data is available as evidence of research.

III. Proportionality and Data Minimization.

MSF will only collect, use and transfer the minimum amount of data that is necessary in relation to the specific purpose(s) pursued. For example:

a) Data collected must be relevant and pertinent to the specific, legitimate activity, not just deemed "interesting". In addition, each time the data is used or transferred the amount of data used/transferred must be necessary and not excessive. For example, this might lead to parts of data sets being stored locally with the necessary safeguards in place (like patient names and highly sensitive data) whilst the rest is transferred to another location for storage.
b) Access to data should be regulated and limited, both in terms of granting access to the minimum number of persons necessary and in terms of only granting access to the parts of the data sets they need to make decisions/ do their job.

IV. Medical Confidentiality and Privacy.

Medical confidentiality (the duty to keep a patient's personal information private which applies not just to doctors but more broadly to all humanitarian workers handling patient and community data) and respecting the right to privacy are essential preconditions for patients' safety and trust; and ensure access to people affected by situations of armed conflict, epidemics, healthcare exclusion and natural or man-made disasters, proximity to people in need, the safety of MSF staff and the ongoing viability of MSF's humanitarian action.

For data collected for the health care or vital interests of a person: without prior patient consent, MSF will not disclose identifiable data or data that could cause harm to any persons or entities that are not *directly* involved in the management of the patient(s)/communities and who need to access the data in order to perform their assignment. Where such data is to be used in research, MSF will comply with the protections outlined in the *Specific Considerations* below.

For data collected for health research: MSF shall strictly respect medical confidentiality and shall only disclose data to persons and entities when the appropriate safeguards are in place and in accordance with applicable ethical and legal rules (see *Specific Considerations* below).

For data collected for communication and advocacy: MSF shall only disclose identifiable data to persons and entities with the patient's consent and the appropriate safeguards in place, recognizing that communication and advocacy data can be very sensitive when embedded in MSF programs and therefore that the strictest application of these principles should apply.

In all cases: MSF shall carefully and systematically assess whether any legal obligation to disclose data may put the patient, identified groups or communities at risk of harm, recognizing that MSF operates in contexts where there are often no appropriate safeguards or protection mechanisms. Notably, this concerns when the best interests of the patient are at stake and national compulsory notification rules for:

a) patient identifiable information from which an implication of criminal conduct could be drawn; for example, data related to violence (bullet wounds or sexual violence);
b) diseases that are notifiable under public health legislation (for example, TB, HIV, Ebola and diseases with potential to cause epidemics);
c) when authorities make a requisition for or ask to access patient data for law enforcement or intelligence purposes in situations of an armed conflict or violence, where the authority requiring access represents a party to the conflict or when the nature of the data could lead to discrimination or prosecution.

Where a possible risk or harm is identified, MSF shall use best endeavours to implement necessary precautions and mitigating factors to protect exposed individuals or communities.

V. Do no harm.

Inappropriate collection, unauthorized use, disclosure of, or access to, patient or community data, **may result in harm** to the very individuals and populations MSF aims to assist, MSF staff or MSF's humanitarian action; especially when the data is highly sensitive (for example, data relating to violence, abuse, coercion and deprivation). In practice, risks may range from physical, mental, dignitary, financial, political and legal harm or threats of harm, discrimination, social marginalisation, and stigmatisation, and are often not foreseen by the individual soliciting the information, or the person providing it. For example, in certain situations, people providing information may face reprisals regardless of what information is shared, merely for sharing data.

MSF will systematically: screen for and identify any data that could be high risk before any collection; and assess the risk, for an individual, group, MSF or its staff in collecting, using or transferring such data (including for storage, archiving, and handover, transfer or destruction upon MSF departure from a program). In some cases, it may be appropriate to refrain from the operation in the first place. In all cases, if the data collection, use or transfer goes ahead, MSF will make explicit the appropriate safeguards needed and ensure they are implemented.

VI. Transparency and Respect for Patients.

MSF shall be transparent with patients with regards to their data and MSF's data management policies and practices: patients are entitled to make informed decisions. MSF shall provide all relevant facts for patients to be able to evaluate and understand the consequences of them sharing their data with MSF. Importantly, MSF shall give notice of:

a) who MSF is;
b) the specific purpose(s) MSF collects information for, if it is not solely for their care;
c) who will have access to the information they share with MSF in case this goes beyond their direct caregiver, on what basis and for what reason; and
d) where MSF is collecting large cohort data or data it reasonably knows will be used in research, notification that de-identified data may be used or shared for statistical, historical or research purposes in accordance with all applicable legal and ethical rules.

Any information and communication given to patients and communities should be easily accessible and easy to understand, which implies providing translations where necessary, and using clear and plain language. The format and mode of information provided will also have to be flexible, recognizing the emergency nature of a lot of MSF's work.

Patients must also be proactively made aware they can refuse to participate in any MSF activity. In particular, whenever data is collected for health research, advocacy, communication or operational purposes in settings where MSF also carries out health care, patients shall be explicitly informed that their participation, or not, shall not affect their right to any health services they may otherwise be entitled to.

To the extent reasonably possible, patients must be able to **access** and **correct** their identifiable data. Individuals can also request **deletion** of their identifiable data and/or **object** to MSF's collection, use or transfer of it.

Informed consent

MSF has to seek informed consent for a number of medical, good clinical practice, research, advocacy, ethical and legal reasons. MSF shall endeavour to put the necessary measures in place to ensure valid consent is obtained, recognizing in the contexts in which MSF often operates, and given the situation of need and vulnerability of most MSF patients, *it can be difficult to fulfil the basic conditions of valid consent, in particular that it is informed and freely given*.

MSF shall take into account: the asymmetrical nature of the patient–humanitarian worker relationship; the lack of alternative to the specific assistance being offered; when (new) technologies are involved, with multiple data flows and multiple stakeholders, the difficulty for individuals to fully appreciate the risks and benefits of how his/ her data will be managed and disseminated.

Whenever possible, MSF shall endeavor to mitigate the limits of consent; for example and when appropriate, by distancing as much as possible activities relative to assistance (health care, distribution of non-food items) with other MSF activities based on consent and that are not directly related to assistance (for example, research, advocacy and communication). For example, by having different personnel performing clinical and research activities; not taking consent for advocacy or communication purposes inside MSF clinics; refraining from engaging in data collection if conditions for free and informed consent are too poor; or collecting only anonymous data from the start as an alternative.

Where data is used in research, MSF will also comply with the consent considerations outlined in the *Specific Considerations* below. Where data is shared with third parties, MSF will also comply with the considerations in the MSF Data Sharing Policy.

MSF will make every effort to ensure that patients and groups with heightened risks, including minors, women and the elderly, are fully counted and adequately represented in MSF data and that their heightened risks are addressed. In cases involving children, MSF will take into consideration their evolving capacities and involve both the child and the child's parent or guardian, except in those cases in which informing the parents or caregivers could put the child at risk (of retaliation, violence, abuse and/or neglect). Persons with disabilities may need and therefore shall be given specific support based on the nature of their disability.

VII. Security.

Data will be protected from improper disclosure, undue use, copy or transfer, unauthorized modifications or tampering, and accidental or unlawful destruction or loss. Data collected will also be stored in a safe way so that it can be accessed only by authorized personnel.

MSF shall assess the risks at each site where data is collected, used and transferred and implement security measures to mitigate against risks according to: the type of data collected and the nature, scope, context and purposes of the data operation; the potential to cause harm if the data is handled inappropriately; and the medium on which the data is collected and stored.

Analyzing the security measures is an ongoing process which takes into account technological and software developments (the state of the art) and the costs of implementation. It also incorporates the need for incident response plans to handle any breaches of this policy's principles.

VIII. Accuracy.

Accurate and complete data is essential to ensuring good health care to patients, there are numerous risks to patients if inaccurate data is processed and used. Therefore, MSF will take all reasonable steps to ensure the data collected is truthful, kept accurate and, where necessary, kept up to date. MSF will make efforts to ensure the reliability and integrity of patient data, which begins with the accuracy and the completeness of source data. In certain circumstances, including at the request of a patient, MSF may correct or delete data that is inaccurate, incomplete, unnecessary or excessive.

Conflict of the Principles

There may be instances where principles within this policy appear mutually inconsistent and where a balance between different rights and principles needs to be struck; the best interests of the patient, the principle of *'do no harm'* and health ethics shall guide MSF in arbitrating and balancing the different stakes at play on a case-by-case basis.

Specific Considerations

De-identification of data: In the following situations, MSF will endeavor to anonymise (so that data can never be linked to an individual or small group) or de-identify data (so that the data can only be linked to individuals/ small groups using a code or other technique which is kept secure and separate) as a method of reducing possible risk in case of unauthorized use or disclosure:

- the collection, use and transfer of highly sensitive data;
- the collection, use and transfer of data in research;
- the collection, use and transfer of data in communication and advocacy;
- transfers of data for which identifiers are not essential for the tasks to be performed;
- transfer of data to third parties;
- the collection, use and transfer of large electronic databases or digital data;
- wherever possible and reasonable, digital archiving;
- wherever else deemed necessary in the specific context.

MSF will also consider for highly sensitive data whether it is possible to collect anonymous data from the outset, for example, data collected for communication and advocacy purposes.

1. Data used in Research (including Data Sharing and Secondary Use of Data)

MSF is committed to carrying out research in an open, transparent and accountable manner and in accordance with the principles of all applicable medical confidentiality, privacy, health ethics and health research laws,

regulations and good practices. This includes the do no harm principle, respecting patients' autonomy, patient confidentiality, the patient's right to informed consent and the fair and equitable sharing of benefits.

MSF shall carefully and systematically assess issues of potential harm from use of data in research and shall seek ethical clearance from national ethics committees and the MSF Ethics Review Board as appropriate.

The aim of using patient data in research is to bring wider health benefits to the individuals and communities where MSF operates. MSF does not use patient data for commercial purposes and will use its best efforts to ensure that all results of research are widely disseminated, in a timely manner and do not lead to prohibitively costly approaches, restrictive intellectual property strategies or any other issues that may inhibit or delay the use of the results to the benefit of low and middle-income countries.

In addition to respecting all applicable medical confidentiality, privacy, health ethics and health research laws, regulations and good practices (which set additional requirements to this policy on the use of peoples' data in research), for research involving identifiable data:

a) **Prospective research:** MSF shall carry out prospective research with patient informed consent and MSF shall systematically seek consent for secondary use of de-identified data. If patients "opt out" of secondary use of their de-identified data then no further use of it shall be made.
b) **Retrospective research i.e. secondary use of data for scientific or historical research:** MSF works with neglected populations, on neglected diseases and in very specific contexts for which important knowledge gaps exist including of adapted health models, strategies and medical inventions, drugs, vaccines and diagnostics. Like prospective research, retrospective research is also subject to ethics review. MSF shall perform retrospective research (itself or with others) only when:
    - the use for research is proportionate to the aim pursued;
    - adequate technical and organizational safeguards have been put in place to make sure the minimum amount of data necessary is used/transferred;
    - where informed consent for using data in research was not obtained, an approach to consent and/or waiver of consent is approved by or in accordance with the rules of the responsible ethics committee of the country of the patient or group whose data is concerned and MSF Ethics Review Board; and
    - all other applicable ethical and legal research rules are respected.

Sharing data with third parties for research:

MSF recognizes the ethical imperative it has to share de-identified data openly, transparently and in a timely manner with the appropriate safeguards to support or create evidence for the greater public health good, which needs to rely on good practices in data collection, use and management. As permitted by ethical and legal rules, under certain conditions, MSF may use or share anonymised, de-identified and/or aggregated health information for statistical, historical or scientific purposes, according to the research conditions set out above, the rest of the terms of this MSF Health Data Protection Policy, as well as the terms of the MSF Data Sharing Policy (http://www.msf.org/en/msf-data-sharing-policy).

2. Digital Health

MSF recognizes the increased use of digital health technology, tools, and applications globally (for example, Electronic Medical Records, mobile health applications, telemedicine, drones, robotics, big data analytics, surveillance applications, wearable devices, biometrics and audio and imaging materials). The convergence of

digital technology with healthcare requires special attention as protection of data in digital environments presents new possibilities and complexities as digital health applications collect, use and transfer health data**.**

As MSF begins to adopt digital health tools there are new benefits to patient care as well as new challenges with regards to patient data protection. With easier and faster processing and portability of ever-increasing quantities of patient data this means MSF must take necessary precautions to ensure confidentiality, integrity and availability. MSF recognizes there are specific risks and challenges related to digital health; including enhanced risks of violating basic notions of data protection such as purpose limitation, data minimization or the retention of data for only as long as necessary for the purposes of collection.

MSF shall make efforts to ensure data management (including standards), confidentiality, integrity and security measures are implemented to protect health data collected on digital platforms.

3. Data Transfers

MSF's operational and organizational structure may lead MSF entities to transfer, share and access health data internationally across the MSF movement. Those transfers may cause disruption to the standard level of data protection, increasing risk of confidentiality breaches and harm. Consequently risks must be carefully assessed and mitigated against prior to creating ways of transferring, sharing or accessing health data internationally across the MSF movement and transfers shall be made in consideration of all applicable laws.

The transfer, sharing or access of data to third parties is contingent on compliance with: MSF's medical-legal toolkit for patient referrals; or, for all other transfers, **MSF's Data Sharing Policy** and upon signature of a Material/Data Transfer Agreement specifying the purpose of transfer, permissible uses of the data, minimum data protection and confidentiality standards, terms of retention and destruction and, where the transfer is for research, access and benefit-sharing provisions.

4. Samples

The handling of human samples (for example, blood, semen, saliva, urine and other body fluids or tissue samples) encompasses more than just data protection practices and this policy complements all the fundamental applicable principles, good practices and laws.

Governance, Accountability and Implementation

MSF shall implement technical and organisational measures to ensure its systems are designed from the start to be protective of data. All MSF employees have a duty to ensure MSF patients' rights around the information given to them and to respect the principles of this policy. MSF will also do its best to ensure that external individuals or organizations it works with (partners, public bodies and others) comply with this policy.

This policy has been validated by the Medical Directors and adopted by the Operational Directors of all MSF Operating Centres. The ultimate responsibility for this policy rests with the Medical Directors. The Medical Directors shall always interpret data protection principles in a way that furthers the ultimate objective of MSF's mandate in humanitarian action.

MSF shall set up an internal organization - at both field project and headquarter levels - to ensure: (a) patient data is protected by **default;** and (b) MSF has systems, governance and structures **designed** to ensure MSF is accountable to its patients. When designing a database, drafting a procedure for collecting data or planning any other data operation, all the principles in this policy must be taken into account and incorporated to the greatest extent possible in the database/procedure/operation.

Recognizing that a single policy does not constitute a recipe for ensuring adequate data protection, this document shall be completed by written guidelines, advice, tools and templates on how to implement the principles and standards described in this policy; as well as a strategy for this policy's implementation, including staff sensitization, training and awareness raising. Implementation, specific governance and designated data protection focal points shall be spelled out in writing at each MSF Operating Centre level.

Every 3 years, the Medical Directors shall commission a review of compliance with this policy and the set of resulting minimum standards issued, and seek recommendations on potential updates to the minimum standards. This effort ensures that this policy remains current and relevant, given the changing context in which MSF operates and global developments in data protection standards.

Any questions about this policy or complaints about how MSF handles patient data should be sent to *healthdataprotection@msf.org*.

Annex 1 – Definitions

Identifiable or Personal Data are any subset of data or information that directly or indirectly identifies an individual. It includes data that reasonably could identify an individual. For example, it includes:

- Data that directly identifies individuals e.g. name, ID number, national number, social security number, phone number, household address or household GPS coordinates, biological samples, medical imagery, biometrics and all other techniques designed to directly identify individuals.
- A combination of data that together can reasonably make it possible to identify an individual e.g. the combination of health center name, pregnancy status and HIV status in the context of a region with low HIV prevalence.

De-identified or Pseudonymised Data are data or information that can no longer be attributed to a specific individual without the use of additional information. For example, when variables are replaced by a code so that the data cannot reasonably lead to the identification of an individual without access to a corresponding key which is held separately and securely.

De-identified data are still personal data (because there is still a risk that it can be linked back to the individual) and can still cause harm to individuals and their communities, especially when the data is highly sensitive.

Anonymous or Anonymised Data are data set(s) that do not include any information allowing direct or indirect identification of an individual (and there is no reasonable basis to believe it could). For example: the data is collected in an anonymous format from the outset; or an anonymisation process removes or replaces the identifiable variables by a code and any corresponding key is *permanently destroyed*. Anonymous and anonymised data can still cause harm to individuals and their communities, for example when it is highly sensitive.

Collection, Use and Transfer; or Processing of data covers all operations performed on data and information, including but not limited to its collection, recording, organization, adaptation/alteration, retrieval, consultation, use, access, analysis, collation, transmission, transfer, disclosure, sharing, storage, archiving, destruction or erasure.

Transfer of data includes both:

- the internal transfer, sharing and access of data in the project, nationally and internationally across the MSF movement; and
- the external transfer, sharing and access of data nationally and internationally from MSF to third parties.

Secondary use of data is when data is used for a different purpose to what it was initially collected for. For example, data that is collected for health care and management of MSF health care systems but that is then used in research.