2022

MSF MEDICAL DIRECTOR PLATFORM

MSF: HEALTH RECORDS MANAGEMENT POLICY

POLICY

INTERSECTION DOCUMENT

VALIDATION PLATFORM AND DATE	MedOp
VERSION/REVISION DATE	20 January 2023
PUBLICATION STATUS	Internal
VERSIONS	*1st edition*
LANGUAGES	**EN**, FR, SP, AR
FEEDBACK CONTACT	Daniela Garone (IMC)
IF ELECTRONIC FILE	link

MEDECINS SANS FRONTIERES

1. Statement Of Purpose

As a medical humanitarian organization, Médecins Sans Frontières (MSF) creates, receives, accesses, consults, modifies, amends, maintains, shares, transfers, stores, retains, and disposes of Health Records. Health Records are a confidential compilation of appropriate facts about an individual or community's health history, including any past and present medical conditions, diagnoses, prevention, and treatments, emphasizing the specific events affecting the patient during the current episode of care.

MSF recognizes the importance of maintaining patient confidentiality and the trust patients and communities have in MSF to manage their data in Health Records according to medical ethical principles and legal obligations.

Health Record management is vital to ensuring the quality of care of patients and the communities that MSF serves, as well as the following purposes:

- Delivering safe, evidence-based, holistic, respectful healthcare tailored to the changing needs of different people and communities
- Supporting healthcare delivery and healthcare services, including surveillance, healthcare worker supervision, and quality control
- Enabling medical humanitarian program monitoring and evaluation
- Assessing the health needs and health determinants of patients and the communities MSF serves
- Conducting operational research
- Ensuring respect for patient rights
- Guaranteeing MSF's institutional memory, both medical and operational
- Improving accountability for our medical and operational actions

Mismanagement of Health Records can impact patient care, patient security and safety, public health, MSF decisions about activities and programs, and reporting to the Ministry of Health and other parties.

This Policy sets standards and arrangements governing the management of Health Records held by MSF for as long as legally, medically, and operationally required. This Policy is aligned with and should be implemented in addition to the MSF Health Data Protection Policy.

1.

2. PURPOSE

This Policy aims to:

- Introduce and define the core principles for the management and retention of Health Records as ethically, operationally, and legally required
- Set forth MSF commitments to these core principles
- Ensure adequate governance and set clear roles and responsibilities for Health Records management
- Provide the foundation for the practical implementation of these principles

3. SCOPE OF THIS POLICY:

This Policy applies to:

- **All types of Health Records** in any format (as described in the table below) managed by MSF in health activities, including Health Records managed in collaboration with the Ministry of Health (MoH) or other actors[1] (see also definitions in Annex 1).
- **The entire lifecycle of Health Records** (as defined below)
- **All MSF medical and non-medical staff** with responsibilities for creating, receiving, consulting, modifying, maintaining, securing, retaining, archiving, transferring, and disposing of Health Records.
- **All places where Health Records may be located:** project, coordination, regional support, and headquarters levels, as well as in any other location outside MSF structures, including in the cloud and/or on servers within MSF and external.

TYPE OF HEALTH RECORD	HEALTH RECORD FORMAT
• Patient medical files (see definition below) and health cards and all documents that are part of patient medical files, • All health registers for service management, patient follow-up, screenings • All operational research documents • All questionnaires, case report forms, data sets linked to surveys or assessments (including qualitative and quantitative), or quality control • All medico-legal documents (certificates, attestation of care, consent forms) • All databases related to health activities • All files with the individual patient or community member information from social workers, patient support, or health promotion, including assessments	• Health Records hard copies (stored in paper, plastic, cardboard) • Photographs, slides, and other images • Microform (microfiche or microfilm) • Audio and video material in tapes, cassettes, CD-ROMs, or any other digital support • Computerized and scanned Health Records saved on hard drives, flash drives, servers, DVDs or CDs and any other electronic storage device, SharePoint, OneDrive, EMR software (Electronic Medical Records), web or phone applications

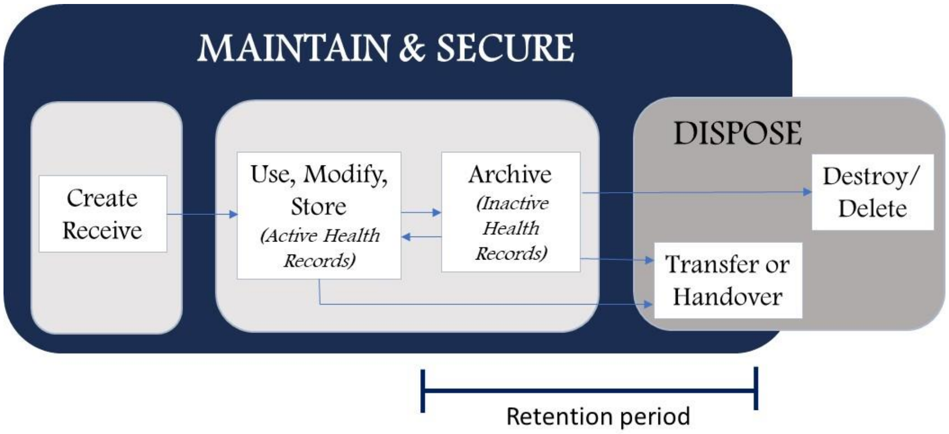
[1] When MSF is working alongside the Ministry of Health or other actors and is not responsible for patient management, MSF is also not responsible for managing Health Records. Nonetheless, MSF must support optimal Health Record management when working with partners.

This policy does not apply to:

- Copies and originals of identity cards, passports, proof of address, or any other personal document belonging to patients, community members, or staff
- Administrative decisions issued by authorities concerning patients, community members, or staff (for instance, birth certificates, asylum decisions, court decisions)
- Consent for advocacy or communication purposes, as well as photos and testimonies collected.
- Health Records attached or embedded in E-mails and social media applications as this should be avoided as much as possible and deleted as soon as possible (separate guidance on emails and Health Record sharing will be provided)

4. Health Record Life Cycle

The lifecycle of Health Records (see illustration below) is composed of the following steps:



1. **Create or receive.** The lifecycle of a Health Record starts at its creation or when it is received from another Party.
2. **Use, modify, and store**. Active Health Records are still used (accessed/consulted/modified/shared) and stored while active.
3. **Archive.** Most Health Records will need to be retained and archived for a specific retention period, once completed or closed and thus inactive.
4. **Maintain and secure.** During their lifecycle, Health Records must be maintained and secured with appropriate classification and organized to protect from unauthorized access and damage while ensuring easy retrieval when required.
5. **Handover or transfer.** Health Records may be transferred to different locations (ex., From project to coordination or HQ) or handed over to the Ministry of Health, another MSF section, or a third party.
6. **Destroy or delete.** At the end of the Retention Period, Health Records and all their copies and duplicates are securely destroyed or deleted, and this destruction/deletion needs to be documented.

5. Core Principles of Health Record Management

The following principles should be applied to the entire life cycle of Health Record management:

- **Beneficence** – the creation, capture, and management of Health Records are integral to MSF medical operational activities and are relevant to the care of a patient or MSF medical-operational health-related program.
- **Minimization** – Health Records shall only contain the minimum relevant and necessary information to ensure quality care is provided to patients and communities. There should be a continuous effort to remove unnecessary and redundant information from Health Records.
- **Quality** – Health Records are complete and accurate. Their information is reliable and reflects the information provided by patients, communities, and relevant health care workers. Health Records should be correct, clear, free of duplication, and reflect the data provided by the actual source.
- **Security** – Health Records will be secure from unauthorized or accidental access, view, alteration, erasure, damage or loss, or unintended threats. Unauthorized or unintentional access, viewing, and disclosure of Health Records will be appropriately monitored, and, when possible (especially with digital tools), audit trails track uses and changes. These incidents must be considered data breaches and treated as per existing reporting and response mechanisms. Health Records will be held in a robust format that remains readable for as long as Health Records are required and need to be retained.
- **Accessibility** – Health Records and the information within them can be efficiently retrieved by those with a legitimate right of access (including upon patient requests) for as long as MSF holds the Health Records.
- **Retention and disposal** –There are consistent and documented retention schedules and storage, archiving, and disposal procedures.
- **Competence** – all staff are knowledgeable about their Health Record-keeping responsibilities through appropriate training and guidance and, if required, further support.
- **Accountability** – adequate Health Records are maintained to account fully and transparently for all actions and decisions while providing healthcare to the patients and communities MSF serves, including support patient centered approach and patient participation in therapeutic decision making. Roles and responsibilities of Health Record management are defined.

In case of conflict or the need to balance any of these principles: the best interests of the patient, the principle of 'do no harm', patient rights, and health ethics shall guide MSF.

6. COMPLIANCE WITH THIS POLICY IMPLIES:

6.1 Health Record Management Core Procedure

All MSF sites (projects, coordination, headquarters, regional support centers) should know the type of Health Records in their care and how they are managed. This is done through mapping, categorization, and inventory. Additionally, Health Records must be retained for a specific duration following legal, regulatory, and operational requirements. Health Records can be archived or transferred/handed over during the retention period. At the end of the retention period, archived Health Records must be destroyed or deleted.

Mapping of Health Records

Mapping of Health Records includes:

- Identifying **all types of Health Records** managed.
- Documenting **the lifecycle**[2] of each type of Health Records.

  This refers to the locations where Health Records are used, transferred, stored, and archived.
- Determining **who has access** to Health Records and with whom Health Records are shared or to whom they are transferred.

Mapping should be done for all sites once this Policy enters into force and systematically updated when starting a new project or activity (medical activity, operational research project, evaluation) as well as when creating a new type of Health Record or handing over or closing a project.

Categorization of Health Records

Categorization will define how the different types of Health Records are managed, notably:

- Level of security and access restrictions,
- Retention schedule and storage/archiving conditions,
- Organization of disposal (transfer, handover, destruction, deletion).

Categorization is done at the creation or reception of Health Records by defining:

1. **The level of sensitivity of Health Records**[3]. Health Data is, per definition, sensitive[4]. Health Records might contain highly sensitive information related to matters that could bring about serious harm to patients or communities if obtained by authorities or armed groups (as defined in the MSF Health Data Protection Policy), such as:
   - Health topics such as violence-related trauma (e.g., torture, sexual and gender-based violence, war wounded), diseases in a context where treatment is mandatory, stigmatized diseases, mental health
   - Interventions that might have significant social or legal consequences, such as safe abortion care or post-abortion care
   - Population or communities served such as people in prisons or detention centers, migrants, or people with specific ethnic origins, political opinions, religious or philosophical beliefs, or sexual orientations
2. **Their retention periods**, that is, how long should a given type of Health Record should be kept when no longer in use and where
3. **To whom they might be transferred or handed over**

Note: Health Records may be a source for secondary purposes such as retrospective operational research. In as much as this is foreseeable (ex., in vertical projects, cohort projects), considering this element in the categorization enables *adapting retention schedules* and *ensuring patients' rights* (to consent to or opt out from having their data used for such purposes).

[2] Examples:
- Patient files created in the emergency ward will be in the inpatient ward until patients are discharged. They are then processed at the data manager's office to support data entry in the inpatient database and archived in a dedicated location of the health structure.
- A contact list (related to an outbreak) created by the surveillance team, transferred to the outreach team for contact follow-up, then moved to the epidemiologist to fill in the register and then stored until the end of the outbreak.

[3] A medico-legal certificate (linked to violence) should be stored in a highly secure location immediately after creation until it can be transferred to the final archiving location.

[4] Most Health Records will contain identifiable information and thus be considered personal data. Aggregated or anonymized Health Records can still be considered highly sensitive if they can be a source of harm to a group of people, a community, staff, or MSF when unlawfully accessed.

INVENTORY OF HEALTH RECORDS

Performing an inventory whereby the quantity and volume of different Health Records are identified is essential to enable the organization of storage, archives, transfer, and destruction/deletion of Health Records.

RETENTION OF HEALTH RECORDS

Each site managing and/or archiving Health Records should have **a retention schedule** for each type of Health Records. This is a clear plan for the retention, archiving, and disposal of Health Records.

The Retention schedule must include the following:

1. **The retention period** of all types of Health Records:

   This refers to how long a Health Record needs to be retained once it is inactive (completed or closed).

   The retention period[5] will depend on the following:

   - The type of Health Record (see categorization section)
   - Country-specific legal or regulatory requirements for retention and destruction of Health Records or, if non-existing, commonly applied requirements.
   - Operational and institutional needs

2. **Information on where and when each type of Health Records is archived and/or disposed** of (transferred or handed over, destroyed or deleted).

ARCHIVING OF HEALTH RECORDS

Each site should have archiving strategies to manage inactive Health Records. This includes:

- Defining the archives' **location(s)** considering the needed size and volume, storage conditions, accessibility, and security (including measures to prevent damage to the archived Health Records by fire, humidity, rodents, and others). Digital Health Records might need to be archived in different locations depending on their initial format or application.
- Defining the **processes of entry**[6], classification, digitalization if needed, registering and reporting access restrictions.
- Defining the **processes of access and retrieval** (upon patient request, upon health care workers' request if patients come back, for quality control or operational research).
- Defining **compliance with retention period and disposal**, including when and to whom to transfer or hand over and when and how to destroy or delete.
- Defining strategies for **handing over the archives to a third party**, including support to set up appropriate locations and archive management when relevant.

DISPOSAL OF HEALTH RECORDS

Disposal of Health Records includes transfer, hand-over, destruction, or deletion.

[5] Some Health Records do not need to be retained and can be destroyed/deleted or given to the patient. Ex. Health card or vaccination card is given to the patient.

[6] Some Health Records will have a short retention period (ex. Screening forms need to be retained until the end of the yearly report period) and may be rather stored at the activity location than in the archiving location.
Other Health Records are particularly sensitive and should be stored in a dedicated space with additional security and access restrictions in the archiving location.

- **Transfer of Health Records** refers to moving the Health Records for further archiving from one site to another, such as from a project to coordination (when archiving is not possible at the project level) or to headquarters (Health Records of survivors of violence or linked to operational research). This means no copies or duplicates remain on the original site.

  The transfer needs to be planned and performed to ensure the safety and security of the Health Records and documented.

- **Hand-over of Health Records** refers to passing the Health Record to the Ministry of Health, another MSF operational center, or any third party taking over the project, medical activity, or archiving. This means no copies or duplicates remain on the original site.
  Hand-over of Health Records should ensure the above-mentioned archiving requirements are met with the support and capacity building of the Ministry of Health or health partner if needed. Before handing over Health Records, patients and the community should be informed that their records might be handed over to another party[7] and given a chance to refuse. In case of the handover of sensitive files (see above), consent should be sought from the patients. A reception certificate needs to be signed by both the MSF site handing over and the receptor of the Health Records.

Note: Transfer of Health Records to a third party not for retention but for other legitimate purposes (such as patient referral, audits, compulsory notification, research, and others) requires the following:

- MSF to keep a copy of the Health Records that will follow the retention schedule
- Patients having given their consent for the transfer of their Health Records
- An agreement (Data Sharing, Data transfer, Research) is signed between MSF and the third party whenever the transfer is not directly linked to individual care

- **At the end of the retention period Health Records must be destroyed or deleted** unless there is a legitimate justification to prolong the retention period, such as a legal case ongoing, validated operational research, audit, or request from the Ministry of Health.
- **Destruction** refers to the physical destruction of hard copies (paper, cardboard) of Health Records beyond any possible reconstruction. In so much, the documents cannot be accessed or read even partially.
- **Deletion** refers to erasing all the soft copies (in any form or application) of Health Records and all their copies, prints, and duplicates in any device or location so much they can no longer be accessed, downloaded, or retrieved.

  Destruction /deletion of Health Records should be documented.

Note: Emergency projects should follow the same rules related to Retention schedules. Retention and archiving of Health Records might be challenging. Still, it must require looking at different solutions such as archiving in an existing project or mission in the country, hand-over to another operational center or Ministry of Health or another party, or the patient or transfer to HQ, all of this depending on the context.

6.2 Governance and Accountability

All MSF staff are responsible for ensuring Health Records are retained in line with this Policy. That good practice is maintained throughout the care of patients and communities MSF serves.

[7] In case it is impossible to reach back to the individual patients, ensure information can be provided through other channels, other healthcare providers or through typical health promotion channels (community involvement, focus group discussions, patient groups, associations, community health workers, radio etc.).

Medical Director and Operations Director	Have the overall responsibility for ensuring that Health Records are managed responsibly within the respective OC's operations.
Medical Coordinators/ Leaders/Heads of Mission	Responsible for ensuring the Policy is implemented in their respective missions and projects, including knowledge of local retention periods and security and access vigilance for paper medical Health Records storage. They will inform Ministries of Health and other collaborating entities on the Policy and general implementation as needed. They will identify and support project-level responsible.
Project-level medical leaders[8]	Responsible for ensuring the medical and non-medical staff are informed, trained, and implementing procedures related to Health Record management, monitoring, and compliance. And report to the medical coordinators.
Medical middle managers in Headquarters and Regional support centers[9]	Responsible for ensuring that the Policy is implemented in their respective locations and that the medical coordinators/project medical leaders are given the necessary information, tools, and support to define, implement and monitor the strategies and procedures established following this Policy in their respective projects.
Record Managers or Data Managers	Support the implementation of the strategies and procedures established following this Policy in their respective projects, missions, and locations and report compliance and implementation results to their medical hierarchy (medical coordinators, medical managers, and project-level medical leaders).
Data Protection Officers (DPO)	Support the privacy risk analysis and provide recommendations in case of Health Records breaches.
Intersectional Legal Department (ILD)	Responsible for advising on national legal frameworks about archiving and retention of Health Records; and supporting the drafting and negotiation of the contracts/agreements needed to record transfers of Health Records.
IT Referents	Responsible for providing support for IT risk assessment for Health Record Management and identifying solutions for mitigations, implementing information security controls
All MSF Staff	Responsible for the safe and appropriate treatment of Health Records to comply with this Policy when managing Health Records.

[8] Depending on project, hospital director or medical director, project medical referent, medical team leader etc.

[9] At the level of the operational and medical department management.

Guidance and tools will be developed or updated for Health Record Management procedures within the whole lifecycle of Health Records (maintaining and securing, mapping, categorization, inventory, retention schedules, archiving, disposal) and the documentation of compliant record-keeping systems. Health Record Management will also be incorporated into basic training, inductions, and field and HQ staff briefings.

7 DEFINITIONS

- **Health data -** any information, recorded in any form or medium, which relates to the physical or mental health of an individual or to the provision of health services to the individual, which reveals details about their health status
- **Patient's medical files (Patient Files)**: used for patient care, including those concerning all specialties, assessment forms, clinical forms, patient's checklists, vital signs forms, prescriptions, referral forms, consultation, and admission reports, medical imagery, laboratory and other investigation results, health workers' notes and follow up sheets, patient's photos-audios- videos. These include mental health files, physiotherapist files, and staff medical files.
- **Social worker's files:** individual files (first assessment and follow-up) from patients/community members or beneficiaries being followed up and supported by a social worker or case manager in the health structure or the community.
- **Hard copy Health Registers:** Paper health registers can be books, folders, or forms that include individual-level data. Paper registers are primarily used at the facility level, though they can serve as inputs to higher-level reporting. There are different types of health registers: health service registers (consultations, patient ward, emergency department, laboratory, pharmacy, etc.), registers linked to pathologies, outbreaks, therapies, pharmacovigilance, and hemovigilance, patient safety incidents, patient follow-up, surveillance or community-based activities, reference keys or golden books (containing both the identifiable information and the code used for pseudonymization).
- **Medico-legal certificates:** written statements from a physician or a qualified health professional who attests to the result of a physical and psychological assessment of a patient.
- **Electronic Health Data:** any database or software in which health data is collected and stored can include excel worksheets, Electronic Medical Records, Health Information Systems, and Access databases. Electronic health data could be stored as identifiable, pseudonymized, or anonymized.
- **Any other document/file/record containing** personal health data, including assessment data, patient safety incident reports, screening results, etc.