• What kind of risk?
• Medical data at MSF Switzerland
• Data and risks
• Common principles applying
• Specific contexts - Emergencies
• Harmonized framework?
• Challenges not yet resolved
Risk perception

• Why protect data?
  – Ensure patients, staff and projects safety
  – Guarantee individuals’ right to medical confidentiality

⇒ Collecting identifying data implies protecting it adequately

• Potential risks
  – Individual penal risks (in case of mis-management)
  – Loss of key information (patient follow-up)
  – Damage to MSF public image (Breach of security)
Generic definitions

• Data for MSF Switzerland
  – Patient files, registers (routine data)
  – Epidemiological data (research), surveys
  – Epidemiological surveillance
  – Laboratory or Biometric samples
  – Medical imaging

• “Data handling” involves
  – Collection, collation, analysis, storage, transfer, archiving, destruction
Medical data collected by MSF

- Paper supports: registers, patient files…
- Electronic format
  - Mostly aggregated data (program monitoring purposes)
  - Individual data for programs centered on 1 pathology (HIV, TB…)
- Move towards more individual data
  - Non-Communicable Diseases, Mental Health
  - Growing appetite for electronic medical records (not implemented yet)
• Personally identifiable data
  – Directly identifiable data
  ⇨ Generally not collected in electronic format for our programs
  – Combination of several data elements leading to individuals’ identification

• Sensitive data: any kind of medical data?
  – Violence-related, disease-related…
  ⇨ Context-dependent (no “hard” classification)
Principles at stake

• Justify data use from the moment it’s collected
• Stick to a minimal set of variables
  ⇒ Potential system impact: manage content centrally
• Patients’ consent
• Confidentiality and security
  ⇒ Protective measures
• Quality assurance to ensure collected data is valid
Specific contexts - Emergencies

• Natural disaster
  – Standardise content but leave it open for changes
  – Ensure frequent data exchanges are possible

• Ebola – Large-scale
  – Data transfer from “restricted” to “open” area
  – Premises organisation must allow oral communication
  – Type of encoding
Data protection & harmonization

• Difficult to reach (internal) consensus on precise rules
  – Define and promote generic principles
  – Illustrate through operational use cases
  ➔ Build a framework
  ➔ Train internal teams

• Data protection is at the crossroad between legal obligations, ethical duties and operational ambitions
Challenges not resolved yet

• Implementation of rules and guidelines at Field level
• Secondary use of data
  – Use of routinely collected data for research purposes
• How to mention / justify data collection in official documents like MoU
• Use of digital files (EMRs)
  – Information becomes ever more portable
  – How to deal with identifiable data?
• Data destruction policy