UNHCR HEALTH INFORMATION SYSTEM

Present & Future

Allen G. K. Maina
Senior Public Health Officer, UNHCR

Roundtable on Beneficiary data: the "poor relation" of the GDPR
GeOnG 2018, Chambery, 29. October 2018
68.5 million forcibly displaced people worldwide

**Internally Displaced People**: 40 million

**Refugees**: 25.4 million

**Asylum-seekers**: 3.1 million

Where the world's displaced people are being hosted:

- **85%**: 85 per cent of the world's displaced people are in developing countries.

- **57%** of refugees worldwide came from three countries:
  - South Sudan: 2.4 m
  - Afghanistan: 2.6 m
  - Syria: 6.3 m

- **Top refugee-hosting countries**:
  - Islamic Republic of Iran: 979,400
  - Lebanon: 10 m
  - Pakistan: 1.6 m
  - Uganda: 1.5 m
  - Turkey: 2.6 m

Number of people newly displaced per day | 2003-2017

10 million **stateless people**

102,800 **Refugees resettled**

44,400 people a day forced to flee their homes because of conflict and persecution

We are funded almost entirely by voluntary contributions, with 87 per cent from governments and the European Union and 10 per cent from private donors.

11,517 staff

We work in 128 countries.
LEGAL AND ETHICAL PERSPECTIVES
Legislation from multiple stakeholders

UNHCR Policies
Data Protection Policy

Regional legislations
GDPR

National legislations
Penal and Civil Code

Partners
Data Sharing Agreements
Given the particularly vulnerable position of persons of concern to UNHCR, the nature of their personal data is generally sensitive and, therefore, requires careful handling.

- Legitimate and fair processing
- Purpose specification
- Necessity and proportionality
- Accuracy
- Respect for the rights of the data subject
- Confidentiality
- Security
- Accountability and supervision
iRHIS

Integrated Refugee Health Information System
Current situation

- Tablet data entry for multiple forms
  - Health
  - WASH
  - Nutrition

- Weekly aggregated synchronization

- One unique web platform for all users (clinicians, Ministries of Health, public) managed with permission rights

→ Electronic equivalent of a register for Ministries of Health

→ Key clinical register for Public Health decisions
Ensure patient-doctor confidentiality

Medical Data in the Health Information System

iRHIS Process

Aggregated data Collection – Entry – Analysis

Individual medical data in the iRHIS remains protected, since it is not being uploaded in the database.

Instead, the iRHIS utilises dedicated data collection, entry and analysis tools that only use aggregate-level data.
Data Protection Assessment

Examples of DPIA aspects planned to be addressed in iRHIS Roll out

<table>
<thead>
<tr>
<th>Data Protection issues &amp; concerns</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data subjects’ rights</td>
<td>Information campaigns to Persons of Concern highlighting their rights</td>
</tr>
<tr>
<td>Accountability &amp; supervision</td>
<td>Modify Data Sharing Agreements with Partners to ensure the implementation of data protection focal points</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>Raise awareness of staff and partners on ICT/office security (including password policies, not leaving documents unattended, not taking documents out of the office, locking offices even for short breaks etc.)</td>
</tr>
<tr>
<td>Relation with stakeholders</td>
<td>Conduct further consultations to address data protection risks with host governments.</td>
</tr>
</tbody>
</table>
Ideas

• The system is only as good as its weakest link - the human who enters the data.
  → User-interfaces must be simple, intuitive and adapted to the workflow, processes and knowledge and skills of the staff.
  → Staff knowledge on data protection and security must be enhanced with specific trainings.

• Less is better: Need to save precious time and effort by avoiding the duplication of systems.
  → Aggregated data from other systems can be entered directly on the web on a weekly/monthly basis in order to integrate with MoH or partners systems.
iRHIS: FUTURE STEPS
Electronic Medical Records

EMR enhances follow up of patients but exponentially increases the quantity of information.

In order to keep a strong data security key aspects need to be addressed;
  • Storage
  • Processing
  • Management

Before thinking on the technical aspects, we need to ensure that all legal and ethical aspects and data protection principles have been assessed and clarified.
Thank you!

Public Health Section
Division of Programme Support and Management
Rue de Montbrillant 94
1202 Geneva, Switzerland

hqphn@unhcr.org