Digital Health Division, Ministry of Health Malawi Data Privacy & Usage Policy for Point of MaHIS app(s)

Version: 2024.0821.0001

Last Updated: 21st August 2024

1.0 - What information we collect

The Digital Health Division (DHD) of the Ministry of Health (MoH) Malawi, hereinafter referred to DHD-MoH, gathers two types of information through its mobile and web versions of the Malawi Healthcare Information System (MaHIS) apps (Electronic Immunization Registry [EIR], Adult Emergency Trauma Centre, eRegister, Outpatient Department [OPD]):

- Personally Identifiable Information (PII) and
- Non-Personally Identifiable Information (Non-PII) .

1.1 Personally Identifiable Information (PII)

PII is information that identifies or can identify you as an individual, such as, but not limited to; Health Identity number, Phone Number(s), email address(es), Name(s), physical address(es).

1.2 Non-Personally Identifiable Information (Non-PII)

Non-PII includes, but is not limited to, Firebase Cloud Messaging tokens, Firebase IDs, IP addresses (both private and public), hardware models, operating system information, software versions, browser information, flight number, vehicle registration number, ship number and any other information that does not reveal your specific identity.

1.2.1 Device Information

We collect information about but not limited to the computers, mobile phones, tablet devices, wearable devices, smart TVs, smart devices and any other web connected devices that use our Apps or integrate with them. This data is combined across different devices that you use. This information is used but not limited to enhancing your user experience, improving features that are device and / or software specific, solving bugs caused by the behaviour of different devices, fraud detection, software update choices amongst others.

1.2.1.1 Device Attributes

Information such as operating system, hardware manufacturer, and hardware model name / number, software versions (of our Apps and dependencies).

1.2.1.2 Network and Connections

Information such as the name of the Mobile Network Operator (MNO) or Internet Service Provider (ISP), private and/or public Internet Protocol (IP) Address (version 4 and/or version 6), connection speed, information about other devices that are nearby or on your network.

2.0 - How Information We Collect Is Used.

2.1 Non-Personally Identifiable Information.

This aggregate information is used as but not limited to usage statistics which helps us track the number of people using the apps, which information is being viewed the most on the apps. Aggregate information may be used in any way approved by the Digital Health Division for trend analyses and analytics that are not yet specified in this policy. In some instances, we may combine Non-PII with PII. If we combine any Non-PII with PII, the combined information will be treated as PII. This "combined" PII is not shared with third parties and is mainly used for analytical purposes which help us improve our Services.

2.2 Personally Identifiable Information

2.2.1 Apps and Sites

Our Apps comply with applicable privacy and security laws of countries where the Services are designed and **officially** distributed. Please note that such sharing may involve the collection, use, storage, disclosure of PII outside the Republic of Malawi.

2.2.2 Communications

We use your PII to send you information related but not limited to the Apps and/or apps installed on your device. This information may be in the form of push notifications delivered via any Cloud Messaging service that we use at any given time. In certain circumstances, we may contact the user directly via their email address(es) and/or phone number(s) to confirm validity and/or receipt of the information.

2.2.3 Administrative Matters

The Digital Health Division reserves the right to contact you in the event of a change in the Ministry of Health's Privacy Policy or to notify you of other administrative matters in connection with any of our Apps and/or services that you are currently using or have once

used. It is the responsibility of the user to provide us with accurate information and to make sure that any changes are understood.

2.2.4 Other Purposes.

We also may disclose your information:

2.2.4.1

In response to a subpoena or similar investigative demand, a court order, or a request for cooperation from law enforcement or another government agency; to establish or exercise our legal rights; to defend against legal claims; or as otherwise required by law. In such cases, we may raise or waive any legal objection or right available to us.

2.2.4.2

When we believe disclosure is appropriate in connection with efforts to investigate, prevent, or take other action regarding illegal activity, suspected fraud or other wrongdoing; to protect and defend the rights, property or safety of our company, our users, our employees, or others; to comply with applicable law or cooperate with law enforcement; or to enforce our website terms and conditions or other agreements or policies.

2.2.4.3

In connection with a substantial corporate transaction, such as the reorganisation or sale of our business, a divestiture, merger, consolidation or asset sale, or in the unlikely event of bankruptcy.

3.0 - App Permissions

The mobile apps make use of user permissions in order to perform functionalities as needed:

3.1 - Camera Permission

The Apps make use of Camera Permissions on Android devices in order to perform the following functions:

- Scan Quick Response (QR) code containing client details on national identity cards and birth certificates.

4.0 - Security of Your PII

Digital Health Division employs reasonable security measures consistent with standard industry practice, for PII collected through any of our Apps, including physical, electronic and operational measures to maintain security and prevent unauthorized access. While the Digital Health Division takes all appropriate steps to safeguard PII under our control, unfortunately, no data transmission over the Internet or method of storing data can be guaranteed to be 100% secure. As such, we cannot guarantee that PII & Non-PII supplied by users will not be accessed on our servers, or intercepted while being transmitted to us over the Internet. We assume no liability for any damages you may suffer as a result of interception, alteration or misuse of information during such transfers. If you have reason to believe that there has been any breach of the security of any of our Apps and/or servers, please contact us immediately at software-developers@kuunika.org

We know it is very important to protect the information you share with us. We take appropriate data and information security measures to help safeguard this information from unauthorised access and disclosure. For example, only authorised employees / consultants / teams are allowed access to Digital Health Division's servers and with appropriate privileges only. Once a UID has been generated, it is used between the application(s) and the server without the need of passing PII. Cloud Messaging tokens are refreshed on a regular basis to avoid intrusion via unnecessary push notifications that could be used by a hacker who has obtained the list of tokens and access key. SSL certificates have been installed on all our servers. We make use of symmetric cryptography to secure data passed in between our Apps.

However, *security is a process and not a product* and no system can be completely secure, we design our Apps with information security as one of the priorities.

5.0 - Offline vs. Online practices

Please note that this Privacy Policy applies solely to our online information gathering and dissemination practices in connection with our Apps, and does not apply to any of our practices conducted offline.

6.0 - Use of Our Apps by Children

Our Apps are not directed to individuals under the age of sixteen (16) without parental consent, and we request that such individuals do not provide PII through any of our Apps. If a parent or guardian becomes aware that his or her child has provided us with personally identifiable information without the parent or guardian’s consent by, for example, misrepresenting his or her age, that parent or guardian should contact us at softwaredevelopers@kuunika.org. If the Digital Health Division determines that it has

collected personal information of children under the age of 13, Digital Health Division will immediately delete such information and any accounts believed to be held by children under 13.

7.0 - Accessing, Updating or Deleting Information Collected About You

Digital Health Division has the right to change any information pertaining to the user, both PII and Non-PII under certain circumstances which warrant such a change as determined by internal team(s) without giving notice to the user. Some information is collected automatically by our Apps and as such it is able to detect a change made by the user and carry out an automatic update. Please note that although this information will not be available on our Apps after you cease to use them, the information may remain stored indefinitely on our servers, both main and backup, and as such we cannot always ensure that these corrections or deletions will reach such other storage facilities in a timely manner.

8.0 - General Data Protection Regulation (GDPR) (EU) 2016/679

Digital Health Division complies with the General Data Protection Regulation (GDPR EU 2016/679) for users who are using our Services and/or Apps and are residents and/or citizens of the countries mentioned in this regulation. Digital Health Division as the Controller of data, reserves the right to store, process, analyse, delete, share, transfer and any other operations deemed fit for business operations and in accordance with this Privacy Policy and best Business Practices.

Data processors working with the Digital Health Division strictly adhere to its policies and guidelines towards the usage, processing and analysing of our shared data. And as such, any data processors found and/or reported to be in breach of our Data Privacy Policy immediately have their Third Party access revoked after a procedural review.

Data subjects have the right to request for their user data to be exported to the Data subject or deleted from our main operational server on which the Service/App is in use.

8.1 - Data Protection Officer

To contact the Data Protection Officer, S/He can be reached at the following address:

Dr. Alinafe Mbewe,

Digital Health Division, Deputy Director

Ministry of Health,

Republic of Malawi

nafekmbewe@gmail.com

NB: Any requests by the Data Subject to the Data Protection Officer should be accompanied with valid identification as well as a signed Affidavit by an authorised legal representative of the country of residence of the Data Subject.

9.0 - Contacting Digital Health Division

The Digital Health Division can be officially contacted via the Deputy Director:

Dr. Alinafe Mbewe,
Digital Health Division, Deputy Director,
Ministry of Health,
Republic of Malawi
nafekmbewe@gmail.com