## APPENDIX A: INTERVENTION IN DETAIL

*Possible* partnered with the non-profit technology company *Medic Mobile* to create a personalized mobile phone-based application for *Possible's* CHWLs. The software was installed on phones through a parallel SIM card (turboSIM) system that allowed for the application to run natively on the phone using Nepali script (Devanagari). Each CHWL was given a basic Samsung 1080t mobile phone and was trained in the use of the software installed on the phone. More details on the technology used can be found in Appendix B.

Prior to the launch of the interventions, the CHWLs would record patient encounter information on paper forms that were prone to inaccuracies and misplacement. During the intervention, CHWLs entered CHW encounter data into the application during their weekly training meetings. The following data fields were collected on the electronic form:

1. Time/Date of Encounter (entered automatically by application)
2. Patient Village Cluster (Programmed into phone, no need for manual entry)
3. Patient Ward (sub-division of Village Cluster)
4. Age
5. Primary Condition (30+ common conditions, entered using hospital coding which can be mapped to ICD9 codes)
6. Gender
7. New/Follow up patient
8. Institution referred to (hospital, local health post, or no additional referral needed)

All text in the application and form was written in Nepali Devanagari script, which is the primary local means of written communication. Writing the program in the local language assisted in the comprehension of the tool.

The application on the mobile phone stored up to twenty messages at a time to be sent later in the case that there was no mobile service. The messages were received by a mobile smart phone that acted as a modem, which in turn uploaded the messages to a netbook running a locally-hosted database. These data were designed to be exported into spreadsheets from which weekly printouts could be created and provided back to each CHWL to show them the conditions in their village cluster, as shown in Figure 2.

One *Medic Mobile* trainer, who spent two weeks at the hospital, installed the system and trained staff and CHWLs. The first step of the training focused on *Possible's* community health and research teams so those staff members would be able to further assist the CHWLs after the trainer left. The trainer then along with *Possible's* Community Health Program director trained the CHWLs, first by describing the purpose of the intervention, then walking them though the application in a hands-on manner. After the trainer departed, supervision of the program and the three-month training period was handed over to hospital staff. *Medic Mobile* employed a full time Nepal Program Director for all *Medic Mobile*-based programs across the country who would visit the hospital every month and as needed, and be available to provide support if any technical issues occurred.

## APPENDIX B: TECHNOLOGY IN DETAIL

*Medic Mobile* employed two software applications during the course of the intervention: Muvuku was the phone-based application which served as the data collection tool and Kujua was the database which received, aggregated, and displayed the data collected through Muvuku.

**Muvuku**:

Muvuku was written in portable C language, and deployed on TurboSIM which is a parallel SIM printed circuit board device produced by Bladox Inc. TurboSIM has 123KiB of flash memory for program and form storage, 4 KiB of RAM, and 4KiB of read-only memory for settings or preferences. Muvuku requires a GSM phone with support for the SIM application tookit, which allows for the TurboSIM app to function. The Muvuku application can store several forms that support a variety of data types, skip logic, reference lists, and validation rules. Data collected is stored in a compressed code by Muvuku and can be sent over standard cellular service via SMS. These SMS messages are read into Kujua and translated into database observations. If Muvuku is not connected to cellular networks, it can save up to 20 completed forms that will be sent when service is next available.

**Kujua:**

In this implementation of the Kujua system, SMS messages sent by Muvuku were received by a low-cost Android phone. SMSsync, an application developed by Ushahidi, was used to accept the SMS messages and transmit them over a local wifi connecton to Kujua which was installed on a low cost netbook. For security purposes, the wifi connection in this implementation was secured and only accessible locally to allow for the uninterrupted transmission of the SMS form results to Kujua.

Kujua is a database system that has the capabilities to collect, aggregate, display, and export data. It was built on Apache's CouchDB software and can run on Windows, Mac or

Linux. Kajua has an installed SMS gateway that allows it to receive and validate SMS messages sent by Muvuku. If the SMS was not sent by a registered phone or if the SMS is not formatted in the Muvuku compressed code format, then the SMS will be rejected and not included in the database. The Kujua database was locally hosted at the hospital for security purposes, but if desired could be hosted online and accessible from outside of the hospital. Kujua features a graphical user interface (GUI) that allows for the collected data to be displayed, and can also export the data in a variety of delimited formats.

**Security:**

When transmitting information on patients, security is of the utmost concern. The data collected by the CHWLs in this intervention did not contain any patient identifiers aside from age, village cluster, and gender, however security precautions were still taken. After a form was sent from Muvuku, it was deleted from the SIMapp's memory. However, one potential liability was if the mobile phone was lost while form data were still stored and waiting to be sent. When sent, the SMS messages were secure and sent through commercial networks before being received by the android phone and transmitted to Kujua. The android phone was password protected, as was the netbook where Kujua was installed. The SMS messages were transmitted from the android phone to Kujua across a secure wifi network, and after receipt, the data was only available locally and protected by additional passwords that only staff involved in the intervention had access to. If more protected information was collected in the intervention, then additional encryption could be applied to the Muvuku and Kujua softwares.