The Utility of Biometric ID in a National eHealth System

An Essential Building Block to Facilitate Universal Health Coverage

Dominic S. Haazen
Lead Health Policy Specialist
Health Nutrition and Population Global Practice
The World Bank
Abuja, Nigeria – April 26, 2018
Content of Presentation

✓ Objectives of a functional integrated eHealth system
✓ Rationale for using biometrics
✓ Biometrics in management and human resources systems
✓ Biometrics in supply chain systems
✓ Biometrics and health insurance systems
✓ Biometrics and clinical systems
✓ Biometrics and patient access to their data
✓ Challenges in incorporating biometrics
✓ Conclusions
Objectives of a functional integrated e-Health system

- Patient-centered – the patient becomes the central subject of the system, including electronic health record, clinical decision support capability and a patient portal to provide access to their own health data and other functions;
- Integrated, responsive and flexible, providing real-time information;
- Interoperable with other systems, including those of the private sector and other health stakeholders such as health insurance funds;
- Used by all levels of the health system: primary care (including community health workers (CHW)), hospital care, public health and social services;
- Provide quality information at all levels that is reliable and timely;
- Respond to the strategic directions of the Ministry of Health to help achieve its short, medium and long-term health objectives
- Be both a clinical and management tool, that meets the needs of health care practitioners, administrators, managers, and directors
Components of an integrated eHealth system

Level:
- Primary (and CHW)
- Hospital
- Health Insurance
- Public Health
- Region/District
- Central

Legend:
- Patient data
- Management data
- Insurance data

Schedule medical appointments, reminders via SMS
Public Portal
Access to health promotion information, statistics, and financial and performance data for the health system

Management System
Clinical Systems & Electronic Patient Record
Private Clinic Systems
Private Hospital Systems
Health Insurance Systems
Surveillance Systems (CD/NCD)
Disease Registries
Human Resources
Drugs/Supplies System

Anonymous patient information and activity data
Notifiable disease information
Disease registry info
Claims information
Information on births and deaths to CRVS agency
Rationale for using biometrics

- **Speed of access and ease of use leading to operational efficiencies**
  - Biometric identification is easy to use and can quickly identify individuals
  - User do not need to be literate to utilize the technology
  - Biometric characteristics are generally stable over time
- **Facilitate access in a secure way**
  - Allows access to systems and physical locations and authenticate users
  - Allows the identification and authentication of those eligible to receive services
  - Provides permission to access personal information
  - Eliminates/reduces need for paper-based IDs
- **Increase security and reduce fraud**
  - Reduce the need for passwords that may be written down or forgotten
  - Increase privacy of personal information by reducing the need to disclose it
  - Allows access to information to be monitored
  - Positively identify those receiving services or coverage
Biometrics in management and human resources systems

• Access control to physical locations and resources
  • Authenticate and control access to facilities
  • Control/record access in restricted areas (OR, ICU, etc.)

• Access control to administrative systems
  • Positively identify those accessing or making modifications to systems
  • Provide audit trail for system updates and other modifications

• Reduce fraud and “ghost workers”
  • Guinea implemented biometric identification of civil servants (including in the health sector) to register all government employees, resulting in the identification of about 11,000 ghost workers (11% of the total), and saving and estimated $20 million annually

• Time and attendance management
  • Mauritius uses fingerprint identification to record time and attendance for civil servants
  • India has developed a biometric attendance system for civil servants, linked to Aadhaar – data is transparent and available on-line
Biometrics in supply chain systems

- **Existing approaches**
  - Biometric access to medical dispensing cabinets, pharmacies
  - Biometric authentication for prescribing controlled substances
  - Positively identify patients prior to medication administration
  - Biometric fingerprint sensors help track vaccination patients
    - Currently implemented in Benin, Kenya, Uganda and Zambia

- **Approaches under development**
  - Using biometric identification of health workers and (possibly) patients to record the receipt and distribution of medications
  - Bar codes on incoming drugs are scanned, together with health worker ID, and data is stored on the blockchain; when medicine is dispensed, bar code as well as worker and patient ID are scanned, and this is also recorded on the blockchain
  - Proof of concept currently being developed by World Bank Blockchain Lab
Biometrics and health insurance (1)

- **Insurance eligibility verification**
  - Gabon CNAMGS Electronic Registration Cards
    - Cards include civil data, a photograph of the holder, and two digitized fingerprints within the microprocessor ensure encryption and protection of the data.
    - Fingerprint sensors used in health facilities to verify eligibility while protecting the confidentiality of personal data.
  - India RSBY
    - Families are issued a biometric enabled smart card containing their fingerprints and photographs.
    - Card ensures that only real beneficiaries can use the smart card and access insured services.
  - Ghana NHIS
    - Biometric verification at health provider introduced – expected to significantly reduce fraud

- **Insurance registration and unique identification**
  - Ghana NHIS
    - In 2013, the NHIS had 26 million names in their registration database – 2 million more than the population of Ghana – currently 7.5 million registered with biometrics and no duplications
Biometrics and health insurance (2)

• **Premium collection**
  * Kenya NHIF
    – Biometric national ID card is needed to create an M-Pesa mobile money account, which can be used to make premium payments.

• **Claims processing and payments**
  * Ghana NHIS
    – Identity of member is biometrically authenticated when they seek medical care, and that identity is linked identity to any claim made by the provider on their behalf.
    – A positive match generates a unique 13-digit claim verification code (CVC), which the provider adds to the claim form as a biometric signature along with the member’s ID, the health provider’s ID and other details. Because the CVC can only be generated in the case of a live fingerprint match, it acts as a vital proof of presence to the insurer, demonstrating that the patient was actually there when the claim was made, and ensuring that the claim is valid.
    – Verification is done through 3,000 biometric verification devices by health providers across the country.
  * Chile I-Med
    – Patients pay copayment electronically using a fingerprint at the doctor’s office.
Biometrics and clinical systems

• **Access control for patient information**
  - Linking fingerprints to EHR can eliminate the need for patients to carry ID, reduce errors from manually copying patient ID numbers, and decrease processing time.
  - Biometrics can also be used to access the EHR when the patient is not conscious, such as in a pre-hospital care or emergency room setting.

• **Authentication and access control of health providers**
  - Biometric technology has shown to be a reliable user authentication mechanism – it restricts delegation of access rights and discourages fraudulent access or impersonation of users.
  - It also facilitates remote access to EHRs by using a biometric feature as a method of authentication, while maintaining a record of access and/or modification of health records.

• **Biometric encryption to increase security of health data**
  - Sensitive information can be encrypted based on a biometric feature making the information available only to the person that possesses the relevant biometric characteristic.
Biometrics and patient access to their data

- **Access control to patient information**
  - Patients can have access to their personal information (either remotely or at a health facility) by using a biometric feature such as fingerprint.
  - The biometric scanner will be able to capture an image of the biometric feature and send it to a centralized system for verification purposes.
  - The image is matched with the stored biometric profile of the patient.
  - When the identity of the patient is verified the system sends back the information originally requested by the patient.

- **Authentication and access control for eHealth services**
  - Biometric technology can be used to access appointment scheduling and other services when accessing a patient portal.
Challenges in incorporating biometrics

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Potential Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Potential false positives and negatives</td>
<td>High quality sensors, multi-modal or two-factor identification</td>
</tr>
<tr>
<td>Potential hacking of biometric database</td>
<td>Encrypt sensors, store encrypted digital representations rather than biometric images.</td>
</tr>
<tr>
<td>Resistance by employees/patients due to concerns about privacy or cultural issues</td>
<td>Communications highlighting the benefits (ease of use, security)</td>
</tr>
<tr>
<td></td>
<td>Offer alternative modalities that are considered more culturally appropriate</td>
</tr>
<tr>
<td>Cost/logistics of setting up biometrics infrastructure and related databases</td>
<td>Biometrics-as-a-Service (BaaS) cloud-based solutions</td>
</tr>
<tr>
<td>Integration with existing eHealth applications</td>
<td>BaaS (and variants), biometrics also already incorporated into many commercial and even open source eHealth modules (e.g. OpenMRS)</td>
</tr>
<tr>
<td>Potential destruction of biometric sensors to obstruct accountability</td>
<td>Multi-functional approaches (e.g., same sensor for time/attendance and access to patient records)</td>
</tr>
</tbody>
</table>
Conclusions

✓ Biometric technology can be used in all parts of a national eHealth system – whether the system is integrated or not.

✓ There are advantages to using biometrics compared to current methods of identification and authentication.

✓ A number of issues still exist with current technological solutions, and their integration the into existing eHealth system, so these issues will need to be considered.

✓ In developing country contexts, issues of access to electricity as well as internet connectivity also need to be addressed.

✓ Nevertheless, good examples of innovation using biometric technology exist across a number of developing countries, and many additional options are being actively explored.
Thank you