Using Biometrics to fight COVID-19

COVID ACTION

UKaid
from the British people

Acknowledgements

This paper was co-authored by Sarah Grieves, Simprints and Siobhan Green, IMC Worldwide, with substantial support from Jessica Studer and Kelly Church (IMC Worldwide) and was made possible through a grant from COVIDAction.

We would like to thank all of the people who reviewed earlier drafts of this paper and gave invaluable feedback, including Moses Dlamini, Sam Jefferies, Craig Jolley, Sarah Parnell, Amy Paul, Rebecca Saxton-Fox, Clayton Sims, Emrys Schoemaker, Norbert Trosien and Nathan Volk.

Disclaimer: The views expressed in this report are those of the authors. This material has been funded by UK aid from the UK government as a part of the Ideas to Impact Programme; however, the views expressed do not necessarily reflect the UK government's official policies, nor those of any of the individuals and organisations referred to in the report.

Abstract

This white paper will discuss how biometrics can be used responsibly for the COVID-19 response, focusing on the use cases of vaccine delivery, clinical trials, and aid delivery. By responsibly, we mean balancing the tensions between optimised usage of biometrics to provide quality services to beneficiaries and improve programming (including reducing fraud and waste), with protecting the privacy and security of beneficiaries and programme implementers while also promoting transparency, openness, and accountability in the use of biometrics.

This white paper covers the following topics

1. A short summary of biometrics (definitions, types, and usage) and COVID-19
2. Review of how biometrics can be and are used for COVID-19
3. Review of potential benefits for biometrics for COVID-19
4. Review of pre-conditions and possible risks to manage
5. Final guidance on how to use biometrics responsibly for COVID-19
6. Proposed metrics around a biometric intervention

1. INTRODUCTION

Context: Increased demand for technology responses for COVID-19

COVID-19 has disrupted nearly every aspect of modern life. The virus has spread to over 200 countries and territories, infected over 100 million people, and claimed over two million lives. In low- and middle-income countries (LMICs), COVID-19 has halted routine healthcare delivery, increased the loss of livelihoods and lives, and exacerbated existing inequities in the countries with the fewest resources to address them. The nature of the virus - its lack of regard for borders and geography - means that tackling its effects in LMICs is of pressing concern for all countries worldwide.

In response to the crisis, a range of technologies, such as chatbots to tackle misinformation about the virus, and cold chain monitoring to ensure that precious vaccines are transported securely, are being deployed by governments, NGOs, and businesses as part of the response efforts. Another technology has been highlighted as a potential game changer for pandemic response: biometrics.

Identification Security Basics

It is important to outline the differences between identification and verification of identity. For **identification**, an individual's identity is being matched with an existing dataset to say who this person is. This match will have a range of confidence based on the biometric, quality of the system, and the existing dataset. For example, the FBI's fingerprint database (AFIS) is routinely used by law enforcement to identify suspects based on fingerprint information captured via different government agencies (including immigration records).

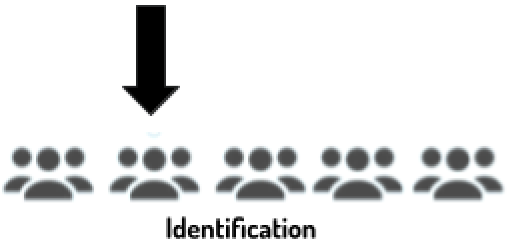

Figure 1: Identifying a group of people [credit: Siobhan Green]

Verification is when someone is stating they are a specific individual, and the biometric system verifies this identity. For example, your phone or laptop may store your fingerprint as a way to lock the device. You are verifying that you are the device owner when you put your finger on the sensor.

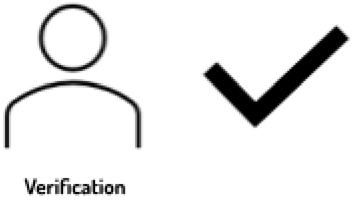

Figure 2: Verifying identity [credit: Siobhan Green]

Ideal multi-factor authentication systems will have a combination of identification forms, summarised as

- Something you know – a password, pin, or security code
- Something you have – a phone, physical card, or token
- Something you are – a biometric characteristic

It is recommended that identification systems use at least two of the three above, depending on the specific contexts of the identification systems.

What are biometrics?

Biometrics are a way to identify who you are or verify that you who you say you are, through measurements of biological characteristics. These characteristics can be physiological (e.g., fingerprints or iris) or behavioural (e.g., voice or gait). There are many different biometric methods depending on what is measured: fingerprints, face, iris, retina, palm, palm veins, voice, signature, gait, etc. Two or more different methods may be combined into a multimodal biometric system.

Figure 3: Different biometric methods [credits: Simprints]

There is no single “best” biometric method as each offer has advantages and disadvantages, especially when working with specific populations and in specific contexts. It is critical to choose a technology that will work effectively in the specific contexts to prevent people from being misidentified or even excluded from services due to a failure of the biometric technology used.

For example, the accuracy of some (but not all) visual biometrics may be affected by unpredictable light levels. Some biometric methods, such as iris scanning, may require specialised hardware that may be harder to maintain in low resource environments. Fingerprint technology may be less accurate for the worn fingerprints of manual labourers, for example, or for people whose fingerprints have been damaged from regular handling of hot cooking implements. Some of the main facial recognition algorithms were shown to have radically different levels of accuracy with people of different racial backgrounds.

It is also important to consider the cultural acceptability of methods that may require users to touch a device (such as fingerprint), or which use an image of a person’s face, as this varies widely across different communities and cultures. A study in Bangladesh found that the majority of veiled Muslim women were willing to provide a fingerprint (although over 70% objected to having their iris scanned or photograph taken). Conversely, less than half of a group of female sex workers in Zambia were comfortable providing their fingerprint, as fingerprints are often associated with law enforcement. The cultural context can also change rapidly due to outside factors, such as the use of biometrics for national identification programmes.

It is therefore important to choose biometric technologies that are calibrated for the population in question, monitor the collection of this data to identify potential exclusions, and try to choose a method which is least likely to lead to exclusion or discriminatory outcomes.

How Biometrics are Used for Humanitarian Assistance and Development

Accurate beneficiary identification is a fundamental building block for every intervention across healthcare, finance, education, and more.

Yet, one billion people have no formal identity, making them invisible in the eyes of the world. This fact is exacerbated in situations of refugee populations, undocumented immigrants, and in times of conflict. Even in countries or populations where formal identification is high, some data, such as for health or political opposition or those in marginalised communities, privacy protection may require a “delinking” of their case data from a government-issued identification number.

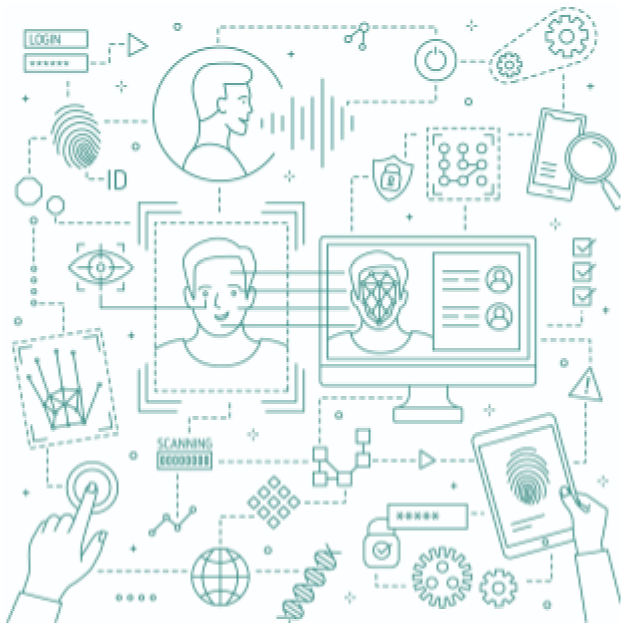

Figure 4: Biometric methods [credits: Adobe photos]

Many traditional approaches for health identifiers have significant flaws. Using personal identifiers including names, date of birth, and postcodes are often not culturally appropriate as many names are very common, people may not know their exact date of birth, many parts of the world do not use postcodes, and/or people may use different names in different contexts for cultural or privacy reasons. Programme-specific tracking tools like vaccination cards, physical QR codes, and patient booklets carried by beneficiaries are often lost or damaged, especially in conflict zones.

In healthcare provision, many organisations use standardised treatment identifiers, such as a HIV treatment ID number or facility IDs. These alphanumeric IDs are used by health care facilities to identify new and return patients for case management. These IDs are usually created by the enrolment facility after the first visit, using a combination of the facility code, date of enrolment, and some personal information (such as initials, month of birth). This code is then used in place of the patient’s name to connect all files across location and time.

While this approach is a good basis for a portable ID linking patient data together, the facility based manual enrolment approach can be very cumbersome and difficult to scale. Facilities may use different formats for their ID format, and countries often do not have a central data repository of all enrollees. Many patients (especially key populations, refugees, and migrants) may visit multiple facilities, creating individual facility IDs for one person. Even when there is a central database, looking up the number may require the patient to remember the date of enrolment or the facility they enrolled in, making linking case management data very challenging and the risk of duplication high.

Biometrics can improve linking while also reducing time and resources

Biometrics as a way to generate unique identifiers have been successful in connecting cases together, verifying delivery of interventions, and improving beneficiary tracking in "last mile" settings. Using a biometric does not require someone to remember information or keep track of a medical record. It can also help link different records together by connecting the same biometric to multiple IDs, reducing fraud and duplications. In addition, biometrics can be used to build solid ID systems in short periods of time, especially in remote areas, sudden migration situations, or when ID cards cannot be a requirement for the delivery of services.

For example, following the deployment of biometric systems, a refugee camp in South Sudan recorded savings of $1 million a month. The World Food Program's SCOPE project has registered 20 million refugees to biometrically verify the distribution of food aid, ensuring the right people are being reached, and also allowing for "better monitoring and risk control".

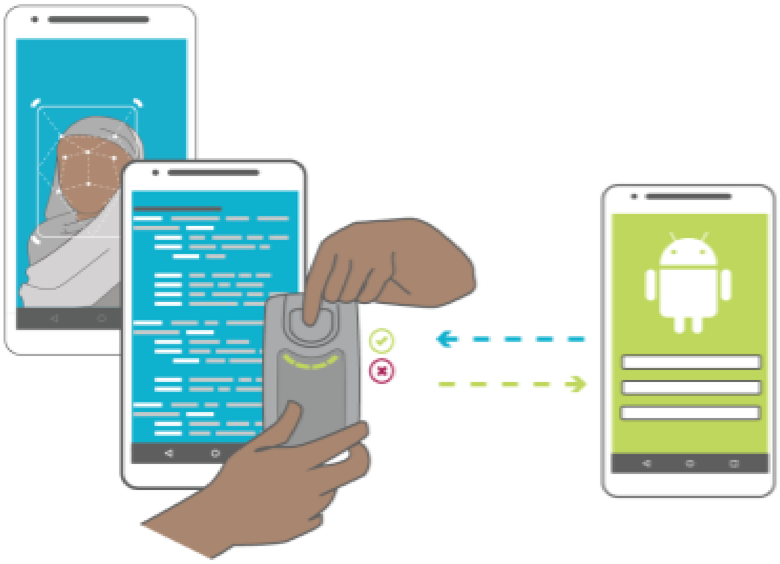

Figure 5: Different biometric methods [credits: Simprints]

However... Biometrics are not a silver bullet

However, biometrics are not a silver bullet; safeguards, planning, and benefit/risk analysis need to be taken into account to determine whether biometrics are appropriate for a specific intervention and to track whether the biometrics continue to offer benefits in rapidly changing conditions.

The strengths of biometrics are often its weaknesses, with some examples below.

Strength	**Weakness**
No need for external token to prove identity (ID card or similar) – harder to "lose", forget, or destroy.	If the biometric data is compromised, "revoking" access via a biometric is very difficult compared to revoking a card (i.e. cannot get new fingerprints).
Biometrics are immutable, meaning they cannot be (easily) changed. This fact means that a biometric identity should last across time in most circumstances.	The fact that biometrics are directly tied to who someone is and cannot be changed puts biometrics into a highly sensitive security category of sensitive personally identifiable information) which will require more security and legal protections around the data.
Biometric identification can be more anonymous when used in a public environment (i.e., not listing a name or an ID code where it could be overheard).	Unless the biometric data is stored completely separately from the user's personal data, a biometric can be used to more closely associate certain personal facts with an individual.
Easier to create unique identifiers across multiple systems using the same biometric, leading to easier case management and tracking of individuals.	Lack of standard calibration or matching standards (or different equipment) may lead to false rejects. It can also lead to combining personal data in ways that could harm an individual (such as using a biometric to match a criminal record to health data or seeking out social services).
Less need to remember a passcode or identification number.	Depending on the calibration or standards, solely using a biometric could lead to false matches (using a 2-factor authentication can help reduce this risk).
Biometrics are widely accessible, not needing literacy or retention of a document.	Some populations are unable to use different biometrics due to physical or cultural conditions, and so may be prevented from accessing services unless a fallback method of identification is available. Children's biometrics may change depending on age and format.

2. BIOMETRICS FOR COVID-19 RESPONSE

Use Case: COVID-19 Vaccinations

Interventions like vaccines are one of the most precious investments in public health and essential to achieving Universal Health Coverage with an ROI of $21 for each dollar of investment. Especially in a pandemic such as COVID-19 with its impacts on economic activity, education, and health, misdirected, duplicate, or insufficient vaccine doses means someone else remains unprotected, as well as increases the likelihood of a nightmare scenario in which viruses develop resistance against limited immunity. Tracking who has received which vaccine is also essential with new variant strains emerging, which show different protections for these different strains.

CHALLENGE - Vaccine Delivery

It is essential we address likely bottlenecks in the delivery of vaccines. Specifically:

- **Verifying delivery of COVID-19 Vaccinations.** Several important vaccines are in relatively short supply, such as HPV (to protect girls and women against cervical cancer) and COVID-19 vaccines. Furthermore, high quality and verified delivery data will be essential to maintaining political will and support from key partners. However, numerous challenges in data quality exist for the delivery of routine immunisations. For example, in Nicaragua, measles coverage calculated based on caregiver recall or child health cards indicated an 82% coverage rate (crude coverage) while dried blood spot samples revealed an effective coverage rate of just 50% (NICS National Brief 2017); while in Nigeria, the gap between administrative data and WHO estimates is almost 34% (WHO & Unicef).
- **Patient tracking for course completion.** To ensure efficacy, it is essential that patients complete course schedules for interventions like immunisations, HIV antiretrovirals, or TB medication. In the case of COVID-19, receiving the second shot *from the same vaccination type* is current best practice. If they don't, the efficacy of these interventions will be reduced, potentially enabling infections and new outbreaks, or worse, antiviral resistance. However, evidence across multiple health interventions in resource-poor settings from vaccines to HIV/AIDs to MNCH consistently highlights patient tracking over time as a key challenge, driven in part by low prevalence of reliable ID. In a study in Lahore, 35% of records were found to be 'unsatisfactory and inaccurate' and 42.5% of the reports either under- or over-reported data (Mahmood and Ayub 2010). To ensure the success of public health campaigns, it will be critical to not only make sure we verify delivery to target populations, but also that we can accurately track whether patients complete their course.

SOLUTION

Biometrics are becoming widely used in development and health programmes to **verify that goods or services reach intended targets**. In a systematic review of over 160 biometric programmes, including routine immunisations in Benin using caregivers' biometrics tied to infant records, Alan Gelb and his colleagues from the Center for Global Development report "The use of biometrics in such programs appears to have improved treatment and programme administration." (Gelb and Clarke 2013). For example, the deployment of biometric registration by the International Organisation for Migration (IOM) in South Sudan brought a reduction of the estimated IDP camp size by 45%, indicating widespread duplication and 'ghost' beneficiaries. As a result, IOM was able to save $1 million a month (Roby). In India, one study that tied caregivers' biometrics to infant immunisation records found that the use of electronic records, direct data capture, and biometric validation may have contributed to the 8% increase in immunisation coverage (Seth et al. 2018).

Similarly, biometrics are increasingly used to ensure treatment adherence and **continuity of care** in health programmes. For example, in a tuberculosis treatment monitoring study in Uganda, lost to follow up rate among biometrically enrolled patients was significantly lower (0%) than that of patients not biometrically enrolled from the previous year (8.8%), leading to the proportion of TB patients with a cured outcome who received biometric monitoring 45% higher than that of patients who did not receive biometric monitoring (Snidal et al. 2015). Biometrics have also been used effectively in vaccine programmes since 2007: a Cholera Vaccine Trial targeting adults in Vietnam found biometrics successfully ensured patient tracking over 8 separate vaccine administrations: "fingerprint scanning for verification of identity during a clinical trial was feasible, reliable, and acceptable in adults in a rural area of Vietnam." (WHO Bulletin 2007).

Figure 6: Indonesian Red Cross (or PMI) uses a digital data collection system

Credit: Musfarayani/IFRC

Use Case: Clinical Trials

CHALLENGE - Clinical Trials

Clinical trials are an important means of testing new COVID-19 vaccinations and other pandemic-specific interventions. However, lack of accurate ID in clinical trials can lead to:

- Cross-contamination between test & control groups, which could make an effective intervention appear ineffective.
- Duplicate enrolments into studies, tying multiple Case Report Forms (CRFs) to a single participant.
- Increased Lost to Follow-up (LTFU) rates, especially for multi-year trials.
- Inability to ultimately assess a drug/vaccine candidates' side effects or effectiveness in specific populations.

SOLUTION

Biometrics can help eliminate cross-contamination between test and control groups, which can otherwise make an effective intervention appear ineffective. For multi-country, multi-site, and/or multi-follow ups trials, unique ID ensures data integrity, especially important for new vaccines like COVID-19. When continuity of care relies on robust ID methods, biometrics can minimise Lost to Follow-up (LTFU) rates. Biometrics can also offer stronger privacy protection for participants than other ID methods do, encouraging sign-ups.

For example, Simprints is a UK-based non-profit developing biometric solutions designed specifically for front-line contexts. Researchers at an East African institution used Simprints to track 12,870 patients in TB/HIV care across clinics to monitor control and intervention arms to improve TB/HIV care. They found no 'contamination' between intervention and control groups, which "is unprecedented". In addition, individual-level data enabled by biometrics allowed researchers to correlate HIV and TB data to specific risk factors for the first time.

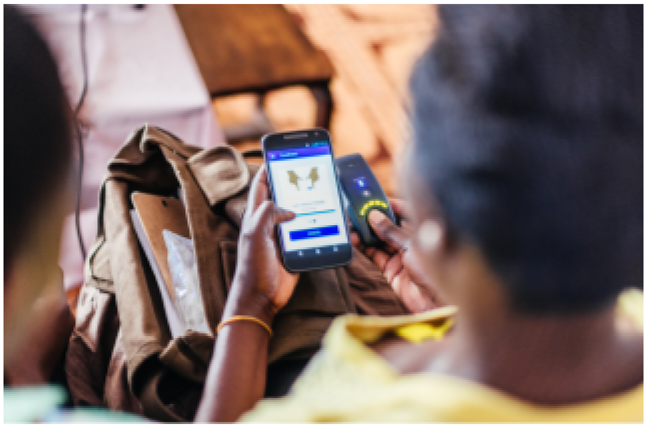

Figure 7: Simprints contact-based fingerprint solution
Credit: Simprints

Use Case: Emergency Aid Distribution

The World Bank estimates that COVID-19 could push more than 18 million people in Sub-Saharan Africa into poverty, and a total of 49 million people around the globe into extreme poverty. Economic growth could contract from 2.4% in 2019 to -5.1% in 2020, bringing about the first recession in 25 years. John Nkengasong, director of the Africa CDC, wrote "the virus could be a national-security crisis first, an economic crisis second, and a health crisis third" if the responses are not calibrated appropriately.

CHALLENGE - Emergency Aid distribution

Without adaptation, existing aid distribution systems may struggle to verify coverage, be susceptible to fraud, miss the intended targeted demographics and risk spreading the virus. During a pandemic, there will be several infrastructure-related problems that may present hurdles to implementing any aid distribution and cash transfer programme. A few examples are:

- **Registration of people is a challenge** because of a need to keep physical distance between people to prevent the spread of the virus
- **Relaxed Know Your Customer (KYC) requirements** in order to distribute the cash/aid faster can cause issues with verifying the recipient

- **Reduced physical contact between staff and participants** voids traditional verification methods like collecting fingerprints and signatures
- **Lack of money agent networks and distribution channels** means cash and aid will need to rely on in-person distribution
- **Ease of 'duping' the system** through **double registrations** in order to receive more aid means the most vulnerable are at risk of missing out.

Cash and aid delivery will only be effective if they can accurately target the households most in need and verify which households are receiving assistance. Furthermore, coordinating this amongst multiple actors will be difficult without a reliable ID, and efforts to ensure that cash and aid is not misdirected will be paramount.

Figure 8: Mobile phone data collection Credit: CALP Network

SOLUTION

Biometrics can ensure:

- Unique registration of participants in the programme
- Unique identification and verification of participants during disbursements
- Programme progress tracking

For example, after deploying a biometrics ID system, the UNHCR found 24% of refugees receiving support in Uganda were "ghosts."

3. POTENTIAL BENEFITS OF BIOMETRICS[1]

As outlined in the above case studies, biometrics can provide benefits to people involved across the spectrum of service delivery in global health programmes, from the patient themselves, through to decision-makers at the policy level.

Area of benefit	Benefit description	Primary benefit for whom					How to maximise this benefit
		Patient	Health worker	Programme Manager & M&E	Policy Maker	Funders & performance managers	
User experience	Ease retrieving records	X	X				Carry out testing of workflow
	Reduced risk of disease transmission via physical ID	X	X			X	Use a contactless biometric modality
	Improved continuity of care	X				X	Ensure robust continuity of care practices are in place e.g. how to follow up after a missed appointment, how to treat a repeat attendee
Data insights	Verification of service delivery and collection of individual-level program data			X			Choose a biometric tool with high accuracy for the population the programme is targeting
	Individual-level programme data			X	X	X	
	Reduction in duplicate records			X	X	X	Export or visualise this data and implement processes to ensure effective use e.g. in programme decision-making
	No mixing between trial			X			

[1] The following two sections use an adapted version of the IMC Worldwide Benefits and Risk Assessment (Church, K., & Green, S. (2021). Benefits and Risk Assessment: How-to Guide for ICT Interventions, Arlington, VA USA. IMC Worldwide).

Area of benefit	Benefit description	Primary benefit for whom					How to maximise this benefit
	and control groups						
Data privacy	No need to use personal identifiers like names	X					Carry out effective community sensitisation to build trust
Cost savings	Reduction in wastage through better resource allocation (e.g., vaccines are delivered in the necessary quantities, and healthcare workers are mobilised to the correct locations).			X		X	Implement continuous improvement practices
	Reduction in fraud			X	X	X	Implement automatic alerts of potentially fraudulent activity
Efficiency	Time saved when retrieving health records	X	X				Choose a biometric tool designed specifically for the setting, to prevent additional time wastage due to technology failures

4. POTENTIAL RISKS OF BIOMETRICS

The table below gives some of the possible risks when using biometrics.

Area of risk	Risk description	Risk to whom					Risk Mitigation Strategy
		Patient*	**Health worker**	**Programme Manager**	**Policy Maker**	**M&E teams**	
Infrastructure feasibility	Technology ineffective due to lack of reliable connectivity	X	X	X	X	X	Choose a biometric solution which works offline (with appropriate data security measures)
	Technology ineffective due to lack of reliable electricity	X	X	X	X	X	Choose a wireless or portable tool, or factor power banks/generators into the project costs
	Technology ineffective in last-mile environment (heat, humidity, unpredictable light conditions)	X	X	X	X	X	Choose a biometric tool designed specifically for the setting
Technology challenges	A beneficiary cannot give biometrics (e.g. due to a lack of fingerprints)	X	X				Implement a process when biometrics cannot be used to ensure access to services
	The algorithm fails to capture biometrics						Choose a biometric tool with high accuracy for the population the programme is targeting, and implement a process when biometrics cannot be used to ensure access to services. Potentially include 2-factor authentication (a PIN or similar that is easy to remember to validate the match).
	A beneficiary is misidentified	X					
Rule of law and access to legal	Limited or non-existent privacy laws	X		X	X		Implement appropriate safeguarding within the project to protect patient privacy.

Area of risk	Risk description	Risk to whom					Risk Mitigation Strategy
recourse							Adhere to strict privacy regulations, even if not required by law.
Patient rights, dignity, and informed consent	A beneficiary refuses to give their biometrics	X	X				Ensure beneficiaries are informed of their rights in an easily-understandable way, and implement a process when biometrics cannot be used to ensure access to services
	A beneficiary is coerced into giving biometrics in order to receive services	X					
	Beneficiaries cannot access their rights due to illiteracy	X	X				
	Personal data is used for purposes other than those originally intended	X					Assess all possible uses for biometric data before data collection begins, so that patients can be informed of their rights. Conduct a Data Protection Impact Assessment Separate biometric data from personal data when feasible so that misuse requires access to both to identify individuals.
Data security	Personal data is leaked, resulting in actual or perceived harm	X		X			Choose appropriate data storage and database encryption options, and create a data security plan which must be followed in the case of a breach Fund proactive monitoring of all biometric systems by IT security experts to be able to identify and respond to potential breaches.
Other	Locked in to one vendor due to a lack of interoperability			X		X	Choose a biometric solution which offers interoperability with other systems and platforms. Use common standards for the

Area of risk	Risk description	Risk to whom					Risk Mitigation Strategy
							biometric database and associated metadata.
	Community resistance to biometric data collection	X	X	X			Carry out effective community sensitisation to build trust. Respect informed consent and not force anyone to use a biometric.

*There may be additional risks when using biometrics with children. Please see UNICEF'S report into biometrics for more detail.

Pre-conditions and considerations for selecting biometrics

Some pre-conditions are needed in order to see the full benefits and reduce the risks of biometrics. It is important that the team understand the following before deciding that a biometric solution will be effective:

- The deployment ecosystem (the power, internet, and available technology devices required to use biometric systems).
- Cultural attitudes towards the biometric being captured or about privacy protection.
- Target demographics to determine if the biometric will need to be highly calibrated (e.g. a population of manual labourers will likely have worn or scarred fingerprints, populations which may be missing fingers or eyes)
- Number of potential beneficiaries to determine the sensitivity level of the biometric. (i.e., greater sensitivity will reduce false positives but may result in more false negatives with improper readings. Less sensitivity may increase false positives but reduce false negatives). A larger number of beneficiaries enrolled in the biometric should consider higher sensitivity, since there will be more close matches.
- The legal and political ecosystem in which biometrics will be deployed to identify potential misuse (by law enforcement or for political purposes, for example).
- Feasible and realistic alternatives in case of a failure of the biometric system and/or lack of consent given.
- System and data security protocols to match risk probability. (i.e., if the biometrics are used on vulnerable populations in which bad actors may want to gain access to the data, higher than normal system security needs to be employed - and the team needs to calculate whether the potential risks outweigh the potential benefits.

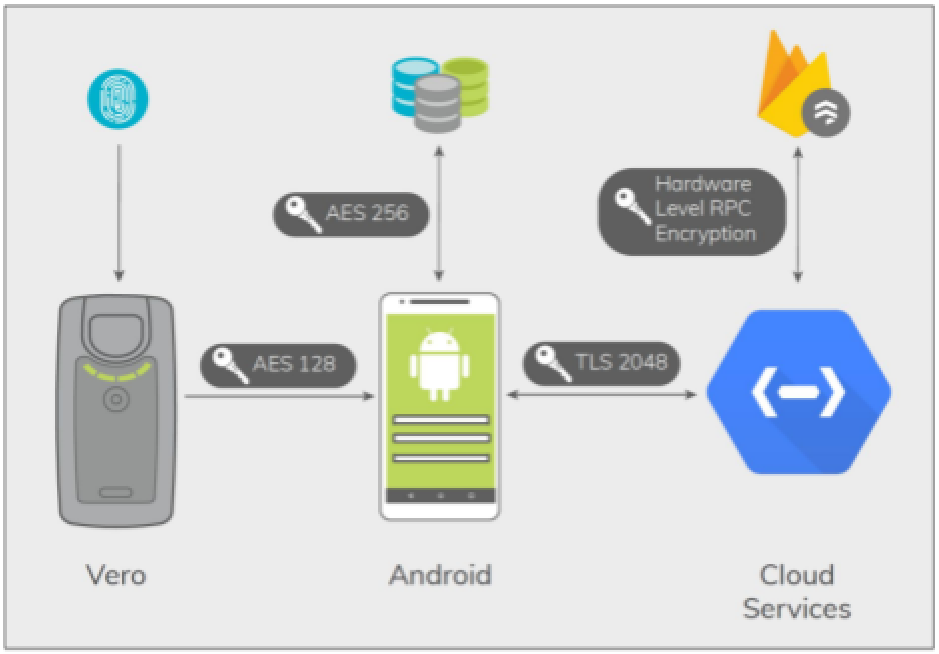

Figure 9: Simprints System Architecture for one fingerprint reader system with encryption between data points [credit: simprints]

Risk Assessment Questions for Biometrics

While the benefits of unique identification through biometrics are manifold, how do we responsibly walk the line between overreaching with its application, and leveraging it as the best tool for the job? Above all, how do we ensure we do no harm to the most vulnerable populations? We can start by asking critical questions around true need, accuracy, privacy and data security, and interoperability.

Is There a Real Need for *Biometric* Unique ID?

Sometimes biometrics isn't the right or best tool for the programme needs. It is worth asking: are existing no-tech identification methods sufficient? If yes, physical IDs with a few key fields like name and date of birth might suffice. Would other lower tech identification methods solve existing challenges? If yes, barcodes or QR codes are viable options. Would the project outcomes be compromised without a reliable, unique ID? If yes, then consider biometrics.

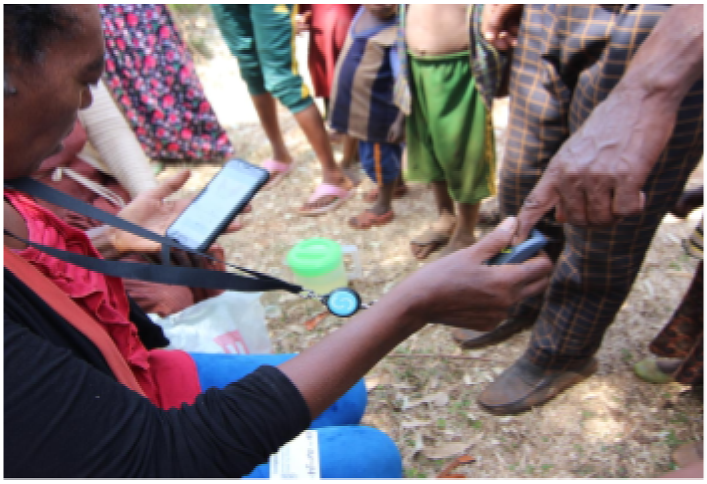

Figure 10: Simprints biometric fingerprint solution [credit: simprints]

Is it Appropriate for the Population you are trying to reach?

Using biometrics in developing country contexts, particularly in low-resource frontline environments, is extremely challenging due to both physiological factors like scarred, worn, or burned fingerprints, and environmental factors like heat, dust, or humidity. Offline functionality may be required in areas of low or no connectivity, and wireless technology is likely to be necessary if power supplies are unreliable. Much of the biometric technology developed to date has focused on working in sterile contexts: indoors and with strong network /internet connectivity, e.g. airports, security, and elections spaces, making it unsuitable for frontline contexts.

It is strongly recommended that for any new roll out of a biometric system include capturing data on failures to enroll, false matches and false rejects, including demographic data (age, gender, occupation, etc) to see if there is any pattern that should be taken into account (i.e. older manual labourers with darker skin have higher levels of failure to enroll than the general population).

Are people's privacy rights respected?

Biometric technology has made it easier to intrude on people's privacy on an unprecedented scale. In many developing countries, privacy laws are limited or even non-existent. Mass biometric enrollments without appropriate safeguarding place individual's civil liberties at risk. As such, keeping biometric data secure and ensuring the privacy rights of individuals are respected must be central to any biometric intervention.

When designing a workflow which includes biometrics, it is important to ask questions such as:

- How can frontline workers explain to beneficiaries what data is being collected, why it's being collected, and how it will be protected?

Some communities will already be relatively familiar with biometric data collection, while others will have no experience of giving their biometrics, and so it is important to make adjustments to the programme accordingly. This could involve customised training for frontline workers, or highly-specific community sensitisation programmes.

- Will beneficiaries understand their rights?

Under the EU's General Data Protection Regulation (GDPR), programmes may use consent as the lawful basis for collecting data about participants. If this is the case, it is critical that participants can give genuine informed consent to have their biometrics taken and stored. A "layered consent protocols" model can help with this: participants will first be given a short notice, designed to be as simple and understandable as possible, even for low-literacy or education populations. This may be followed up with a longer (but still readable) narrative or FAQ to help operators answer any questions raised by beneficiaries. Finally, full legal notices should be available on the app or a website to answer any question about project privacy, regardless of how much or little is required by local regulation.

- What happens if someone does not wish to give their biometrics?

There is no single correct approach to this question, and it is vital that programme implementers plan for this eventuality according to the needs and constraints of their own programmes. For example, a participant may be able to provide another form of ID (such as a name, phone number, or a national ID) in order to access services.

Is the biometric data secure?

By any standard, biometric data is highly sensitive personal information. In fact, GDPR - the world's strictest privacy and security regulation - categorises biometrics as "special category data", alongside sexual orientation, political view, etc. Disregard for data security can lead to large-scale breaches of highly sensitive information, as was found to be the case in the breach of Aadhar in India, compromising the identities of up to one billion people, and similarly a hack exposed more than 8,000 households in West Africa to identity theft.

Biometric data can be stored in a number of ways: raw images, an electronic signature of that image called a "template", or using a method such as hashing or tokenisation, where the sensitive biometric is replaced with a non-sensitive equivalent (Trust Stamp are one vendor taking this approach via their IT^2 technology, which replaces biometric data with their "Irreversibly Transformed Identity Token").

In choosing a storage method, it is important to balance the specific data security and interoperability requirements of the project. The World Bank's ID4D Practitioner's Guide goes into more detail into possible approaches, and notes that "keeping centrally-stored biometrics as templates does not substantially increase security; conversely keeping centrally-stored biometrics as images has additional benefits, such as the ability to generate new templates with a different algorithm".

Keeping this data secure involves a number of factors, including:

1. What *other* personal data are stored with the biometrics - are names, dates of birth, sex, medical histories, and other personal identifiers stored alongside the biometric data?
2. How the database itself is protected - what levels of encryption? Who has access to which levels of security clearance?

Regarding data security, implementers should follow best privacy-by-design practices like using modern data protection standards. An important consideration is **data siloing**, where the biometric provider only stores and processes the biometric data, GPS location, and timestamps, but not the personal data that is linked to each individual for the purposes of the project (e.g. the health data, attendance data, etc.). Conversely, project partners store and process the personal data that needs to be linked with each individual for the purposes of the project, but not the biometric data. Randomly-generated GUIDs are used as the 'bridge' between the two siloed data sets, allowing biometrics to be used to identify individual beneficiaries for the project partner. As long as this data silo approach endures, it should be impossible for the partner to misuse any biometric data or share that data inappropriately, and a breach of the partner's cyber defenses ought not to expose any biometric data. As an added benefit, this approach also serves to limit the impact of a cyber breach of the biometric provider's systems in that the breach would yield multiple pseudo-anonymised numbers (the GUIDs) that are useless without the connected beneficiary information, e.g. names of any beneficiaries or any personal data in health, finance, or education records.

It is also essential to create a security plan in case of breach, which includes, for example, how to remove all access credentials, and a plan for the encryption and removal of all production data.

In addition, external penetration testing can be used to assess security measures and, if necessary, strengthen areas of weakness accordingly.

Is the biometric system interoperable?

The World Bank defines interoperability as "the ability of different functional units—e.g., systems, databases, devices, or applications—to communicate, execute programs, or transfer data in a manner that requires the user to have little or no knowledge of those functional units".

Biometric interoperability refers to the data format that is used to store biometric information. Interoperable biometric data will allow programme implementers to access and re-use biometric data (within the ethical guard-rails discussed above), link multiple modules or services, and exchange vendors (for the whole system or components). Vendor lock-in was the biggest cause of dissatisfaction with technology vendors among African identity authorities, according to the 2018 ID4Africa survey. A lack of interoperability has serious consequences: for example, in Nigeria, the duplicate data capturing and biometric registration exercises in the country have cost the Nigerian government over 208 billion naira (approximately $580 million), wasting precious human and financial resources. Similarly, the use of separate biometric identification systems to register refugees displaced by Boko Haram has led to overlaps in enrolled migratory populations (Roby) between aid agencies.

Biometric data is interoperable if it fulfills two main criteria:

1. The data is stored in a **format** that is defined by an international standard; and
2. The **quality** of the data complies to an international standard

For a detailed description of the different standards that are available, please see the World Bank's ID4D Catalogue of Technical Standards for Digital Identification Systems.

There are a number of interoperability frameworks and platforms available: one example is MOSIP, an open-source modular architecture for building identity systems. Another is OSIA, which is a common set of biometric definitions for the exchange of data between different components of an identity management ecosystem. Both approaches are technology- and vendor-agnostic.

"Interoperability" is not a binary choice but a spectrum, and as discussed previously, it is critical to consider interoperability alongside data privacy and protection. In addition, interoperability requirements will need to be considered in relation to the lead time and budget for a project, the local connectivity and infrastructure, and the existing digital infrastructure.

5. GUIDANCE

Once it has been decided that biometrics may provide value to a programme, below is a checklist to help guide decision-making:

Operational	Technical	Political	Regulatory
Is the workforce familiar with digital technologies? Are there (dis)incentives to use digital tools like biometrics (e.g. will it be seen as a "chore" vs. "efficient")? Which biometric methods will be appropriate? What level of community sensitisation, and with which local leaders, needs to take place before deploying biometrics?	What are the technical systems already in use (e.g. DHIS2, CommCare, OpenSRP)? Who are the key stakeholders involved in further integrating technologies into their health system? How accurate is the technology for the beneficiary population (including accuracy with infants or children where required)? Is the technology robust enough for the environment, and portable enough for the needs of the programme? How will biometric data be stored?	Is there an overarching strategy around digital technologies (either focused on Digital ID or Digital Health Systems) into which biometrics can fold? Is there political will within any relevant levels of government (from senior officials, through to regional and local field officials) to incorporate biometric identity to support vaccination / other areas of health programming?	Is there an ecosystem to support ethical and privacy-first use of biometrics? What will be the process for data protection? What risks exist with regard to misuse of data? What other data is taken alongside biometrics, and is it absolutely necessary for the success of the programme?

Budgeting and Timelines

There are a number of studies that have shown that biometrics are a huge **cost-savings** mechanism. This DFID policy paper gives a number of examples, such as:

- When Nigeria launched its e-ID system, this resulted in an annual saving of $1 billion through exposing 62,000 'ghost workers' in the public sector (a return on investment of nearly 20,000% in one year)
- In the past six years, one billion digital identities have been issued under Aadhaar, India's biometric identification programme, expanding public services to poor and marginalised populations. Cash transfers enabled by Aadhaar are saving around $1 billion per year and it is projected that the benefits of the programme will result in a return of over 52% on investment over 10 years

Direct costs for biometrics vary hugely depending on the biometrics provider chosen, the existing infrastructure, and the features required. Costs typically fall into two categories: setup costs and ongoing costs.

Possible setup costs	Possible ongoing costs
Integration support with existing digital systems Interoperability assessments and support for government systems Custom workflow design and project configuration Data protection and privacy assessments User acceptability testing and materials for community sensitisation campaigns Initial training of users and trainers as well as development of training materials Biometric hardware and project key for mobile applications Access to biometric services for a given number of users, or for a given period of time, on a per-project basis.	Quality assurance and analytics Software maintenance, updates and new features Managed backend service for storage and processing Ongoing project and technical support Fee per user Fee per biometric enrolment / identification

It is important to consider the eventual scale of a programme when considering what kinds of ongoing costs are acceptable. For example, while costs per user or per enrolment may be acceptable for small-scale projects with no opportunity to scale, the costs can very quickly become unsustainable in a larger project. For this reason, a different pricing model may be preferable for a project which will ultimately reach large sections of the population, such as vaccination.

An additional factor to consider is that the ROI of implementing biometrics will increase if it is rolled out across multiple programmes or sectors, reaching higher numbers of beneficiaries. For example, provided that the biometric tools chosen are interoperable (see previous section), an implementing organisation could roll out use of biometrics to link patients to their medical records across multiple touchpoints (vaccination clinics, emergency care, pharmacies etc.), and then increase the ROI even further by extending biometric verification to a cash assistance programme. In situations like this, the “cost per beneficiary” can be extremely low. The graph below gives an example of how this metric can decrease as the total number of beneficiaries increases.

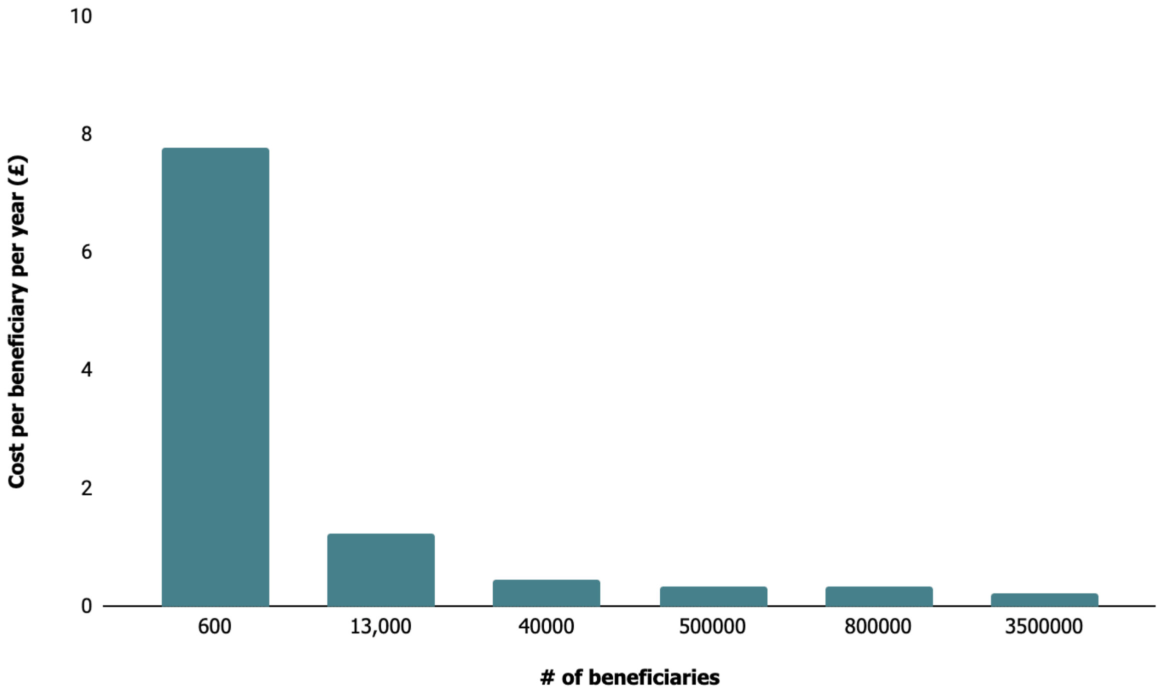

Figure 11: Bar graph of cost per beneficiary per year [credit simprints]

As with costs, the timelines required to implement biometric identification will vary hugely depending on the biometrics provider, the existing infrastructure, and the needs of the programme. For this reason, it is important to consider identification needs as early as possible. Exploring biometrics early not only ensures that there is time to integrate the technology; it also increases the likelihood that biometrics will bring value to the programme, as there is time for risks to be mitigated, for rigorous quality assurance to take place, and for biometrics to be included as an integral part of the programme design, rather than attempting to add it on top of potentially incompatible workflows.

ANNEX 1: METRICS

Below are a selection of metrics that can be used to monitor the benefits, risks and ROI of implementing biometric identification, using a COVID-19 vaccination programme as a use case.

Quantitative:

- Cost saved through deduplication and reduction in resource wastage
- Time taken for the patient authentication process for health workers using biometrics
- Comparison of time taken for patient authentication compared with non-biometric methods
- Number of unique biometric enrolments
- Number of authenticated COVID-19 vaccination events
- Proportion of enrolled patients who receive a full course of vaccines with biometric verification
- Proportion of enrolled patients from vulnerable groups who receive a full course of vaccines with biometric verification
- Number of times the system is unable to enrol of verify a patient, disaggregated by demographic
- Number of patients who refuse biometric enrolment
- Accuracy of the system (true positive and true negative rates)
- Accuracy of the system when face coverings are used

Qualitative:

- Feedback on cultural acceptability of the solution
- Feedback on the user-friendliness of the solution for health workers
- Feedback on the process from patients

Works Cited

Adepetun, Adeyemi. “How Nigeria wastes billions on data capturing | The Guardian Nigeria News - Nigeria and World News — Technology — The Guardian Nigeria News – Nigeria and World News.” *The Guardian Nigeria*, 18 September 2017, https://guardian.ng/technology/how-nigeria-wastes-billions-on-data-capturing/. Accessed 3 December 2021.

Atick, Joseph J., and Niall McCann. “ID4Africa 2017 Conference Publication.” *ID4Africa*, https://www.id4africa.com/2017_event/files/ID4Africa_2017_Conference_Publication.pdf. Accessed 3 December 2021.

Atick, Joseph J., and Zaid Safdar. “World Bank Document.” *World Bank Document*, 11 June 2019, https://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf. Accessed 3 December 2021.

Biometrics Institute. “Types of Biometrics.” *Biometrics Institute*, https://www.biometricsinstitute.org/what-is-biometrics/types-of-biometrics/. Accessed 3 December 2021.

Desai, Vyjayanti T., et al. “The global identification challenge: Who are the 1 billion people without proof of identity?” *World Bank Blogs*, 25 April 2018, https://blogs.worldbank.org/voices/global-identification-challenge-who-are-1-billion-people-without-proof-identity. Accessed 3 December 2021.

The Economist. “Africa is woefully ill-equipped to cope with covid-19.” *The Economist*, 26 March 2020, https://www.economist.com/middle-east-and-africa/2020/03/26/africa-is-woefully-ill-equipped-to-cope-with-covid-19. Accessed 3 December 2021.

Grother, Patrick, et al. "Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects." *National Institute of Standards and Technology Interagency*, vol. Report 8280, 2019. *Face Recognition Vendor Test (FRVT)*, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

International Bank for Reconstruction and Development/The World Bank. "Catalog of Technical Standards for Digital Identification Systems." *World Bank Document*, 2018, https://documents1.worldbank.org/curated/en/707151536126464867/pdf/129743-WP-PUBLIC-ID4D-Catalog-of-Technical-Standards.pdf. Accessed 3 December 2021.

Lindley, Emma, and Stephen Wilson. "The Privacy Protecting Power of IT." *Trust Stamp*, https://truststamp.ai/Whitepaper.html. Accessed 3 December 2021.

Mahler, Daniel G., et al. "The impact of COVID-19 (Coronavirus) on global poverty: Why Sub-Saharan Africa might be the region hardest hit." *World Bank Blogs*, 20 April 2020, https://blogs.worldbank.org/opendata/impact-covid-19-coronavirus-global-poverty-why-sub-saharan-africa-might-be-region-hardest. Accessed 3 December 2021.

MOSIP. "What is a foundational identity system?" *MOSIP*, https://www.mosip.io/about.php. Accessed 3 December 2021.

"1 bn records compromised in Aadhaar breach since January: Gemalto." *The Hindu Business Line*, 20 October 2018, https://www.thehindubusinessline.com/news/1-bn-records-compromised-in-aadhaar-breach-since-january-gemalto/article25224758.ece. Accessed 3 December 2021.

OSIA. "OSIA." *Secure Identity Alliance*, https://secureidentityalliance.org/osia-about. Accessed 3 December 2021.

Parker, Ben. "Audit finds UN refugee agency critically mismanaged donor funds in Uganda." *The New Humanitarian*, 28 November 2018, https://www.thenewhumanitarian.org/news/2018/11/28/audit-finds-un-refugee-agency-critically-mismanaged-donor-funds-uganda. Accessed 3 December 2021.

Parker, Ben. "Security lapses at aid agency leave beneficiary data at risk." *The New Humanitarian*, 27 November 2017, https://www.thenewhumanitarian.org/investigations/2017/11/27/security-lapses-aid-agency-leave-beneficiary-data-risk. Accessed 3 December 2021.

Plata, Gabriel. "Meet the 34 Million People Who Were Never Born." *Inter-American Development Bank*, https://www.iadb.org/en/improvinglives/34-million-people-who-were-never-born. Accessed 3 December 2021.

Roby, Christin. "Biometric registration aids conflict regions, but gaps still exist." *Devex*, 9 October 2017, https://www.devex.com/news/biometric-registration-aids-conflict-regions-but-gaps-still-exist-91117. Accessed 3 December 2021.

Seth R, Akinboyo I, Chhabra A, et al. Mobile Phone Incentives for Childhood Immunizations in Rural India. Pediatrics. 2018;141(4):e20173455

Snidal, Sarah J., et al. "Use of eCompliance, an Innovative Biometric System for Monitoring of Tuberculosis Treatment in Rural Uganda." *The American Journal of Tropical Medicine and Hygiene*, vol. 92, no. 6, 2015, pp. 1271-1279. *The American Journal of Tropical Medicine and Hygiene*, https://www.ajtmh.org/view/journals/tpmd/92/6/article-p1271.xml.

"Understanding and Selecting a Tokenization Solution." *Securosis*, https://securosis.com/assets/library/reports/Securosis_Understanding_Tokenization_V.1_.0_.pdf. Accessed 3 December 2021.

UNICEF. "Biometrics - UNICEF DATA." *UNICEF Data*, July 2019, https://data.unicef.org/resources/biometrics/. Accessed 3 December 2021.

WFP. "WFP SCOPE." *WFP Remote Access Secure Services*, https://documents.wfp.org/stellent/groups/public/documents/communications/wfp258555.pdf. Accessed 3 December 2021.

WHO. “Nigeria: WHO and UNICEF estimates of immunization coverage: 2019 revision.” *WHO | World Health Organization*, https://www.who.int/immunization/monitoring_surveillance/data/nga.pdf. Accessed 3 December 2021.

World Bank.. Technology Landscape for Digital Identification, Washington, DC: World Bank License: Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO). 2018

World Bank: Office of the Chief Economist for the Africa Region. “APRIL 2020 | VOLUME 21.” *Open Knowledge Repository*, 4 April 2020, https://openknowledge.worldbank.org/bitstream/handle/10986/33541/9781464815683.pdf?sequence=18. Accessed 3 December 2021.

Learn more at

medium.com/covidaction

COVID ACTION

UKaid
from the British people