unicef
data for children

Faces, Fingerprints & Feet

Guidance on assessing the value of including biometric technologies in UNICEF-supported programs

July 2019

ACKNOWLEDGEMENTS

This guidance was developed by Nicola Richards (Independent consultant) and a UNICEF project team including:
Karen Carter – Data and Analytics Section; Division of Data, Research and Policy (Project manager)
Kristen Wenz – Child Protection, Programme Division
Tanya Accone – Office of Innovation
Shane Khan – Data and Analytics Section; Division of Data, Research and Policy
Toby Wicks – Data and Analytics Section; Division of Data, Research and Policy
Steven Vosloo – Policy Lab; Division of Data, Research and Policy
Sophie Clavet – Child Safeguarding Unit, Office of the Executive Director.

Valuable input and feedback was also provided by a broad range of UNICEF staff, to whom we extend our appreciation, including the Admin Data Task team, country and regional offices who participated in the interviews and shared their concerns and experiences, and those who provided feedback and comments on earlier drafts. We would also like to acknowledge the valuable insights shared by our colleagues at UNHCR and WFP as this document was formulated.

CONTENTS

GLOSSARY

Age effect	Variation in recognition accuracy between different user groups based on their age at enrolment
Ageing effect	Variation in recognition accuracy due to an increase of time between enrolment and query. Often due to physical changes in the biometric trait (such as fingerprints degrading over time), making matching with saved templates more difficult
Algorithm	Sets of mathematical instructions or rules that, especially if given to a computer, will help to calculate an answer to a problem
Authentication	The process whereby a user claims an identity and the system verifies this claim by comparing the most recent template generated with those already stored, in what is referred to as 'one-to-one' or '1:1' matching (1-3)
Deoxyribonucleic acid (DNA)	DNA is the genetic code that is unique to every individual and has traditionally been used in law enforcement and paternity testing. The technology works by measuring short-term repeat sequences found in the DNA (4)
Failure to acquire (FTA)	This is when the trait provided during enrolment cannot be acquired or processed (for example, when a user does not stare directly into an iris scanner, and so no photos are taken) (3)
Failure to enrol (FTE)	Includes FTA plus all users who are rejected from the system due to the poor-quality of data captured (for example, a blurred photo due to movement during capture) (5)
False accept rate (FAR)	Proportion of individuals who are incorrectly matched to another user's biometric templates
Gallery images	Raw biometric images acquired during enrolment (also referred to as reference, stored or enrolment images)
Identification	During identification, a user attempts to positively identify themselves without explicitly claiming an identity. The biometric data they provide is compared with all templates already stored in the system in 'one-to-many' or '1:N' matching (5)
Matching algorithm	Compares query images with those in the saved template to give match scores on the level of similarity, with a larger score indicating greater similarity (5)
Query images	Images presented during recognition (also referred to as probe or input images)
Rank-1 identification	Proportion of queries where the matched template is correct and provided as the most likely (number one) candidate (5, 6). Authors often also use the Rank-3,-5, or-k rate, which allows for the correct template to be returned in a list of three, five or 'k' top candidates, where 'k' can be any whole number
Template	Compact but expressive digital representation of the biometric trait (5)
Threshold	The level at which a user's identity will be accepted or rejected. Very secure systems have high thresholds, however the level reflects a trade-off between the effectiveness of the system for practical application, against the risk of incorrect recognition (3)
Trait	Bodily characteristics or features used in biometric systems for recognition. Also referred to as 'features' or 'modalities'
True accept rate (TAR)	Measure of the ability of the system to correctly match the biometric trait(s) for the same person. Calculated by the proportion of genuine users who are correctly matched to their biometric templates
Verification	See 'authentication'

INTRODUCTION

Automated biometric recognition systems (simply, 'biometric technologies') – that is, the use of fingerprints, facial recognition, iris scans etc. – are increasingly being used by national governments and partner agencies to identify individuals and manage data in service delivery across a range of sectors. UNHCR and the WFP, for example, have fully integrated biometrics into their cash management programs (7), and more countries are investing in biometric technology linked to national identity systems (8). Private industry has embraced this technology as a means of securing financial transactions and personal devices, with most newer smartphones having inbuilt fingerprint scanners along with facial recognition abilities.

UNICEF has a specific mandate to protect, respect and uphold the rights of children and their families globally, and to help facilitate full implementation of the Universal Declaration of Human Rights and the Convention on the Rights of the Child (CRC) (9); including supporting the establishment of a legal identity at birth. As national identity systems are increasingly being linked to biometric data (for both adults and children), we have an important role to ensure that such systems are linked to civil registration and ensure a 'life-cycle' approach to identification. At the same time, we are also invested in how we identify children across a broad range of functional registers – including health, education and child protection, improving the accountability and effectiveness of our own cash programming, determining when and how we should link data – balancing privacy against the risks of not using data, and how new technologies could help us improve service delivery for better outcomes and improved inclusivity.

While biometric technology is simply an identification tool and does not confer identity in its own right – it does offer a range of potential advantages in UNICEF programs and the government systems we support. To this end, UNICEF has undertaken a limited range of pilot and small-scale projects with the technology across the organization and is increasingly considering what role this technology may play in our broader programming. We are also working closely with partners in the field whose data collection is based on biometrics. While the potential benefits of biometric technologies are relatively clear, there is limited guidance on appropriate applications and how to manage potential risks in a way that specifically ensures the rights of children are protected.

This document provides practical guidance on evaluating when the use of biometric technology may be appropriate, through consideration of potential benefits and risks. The guidance has been created in response to demand from country and regional offices, and strong interest from external partners in understanding how to engage with our work in this area in a responsible manner. The document is guided by existing best practice and evidence, while noting that many key questions are not adequately addressed in the published literature.

The document is divided into five sections. Section one provides important background information, including a brief explanation of biometric technologies and how they work. Section two introduces the benefits, risks and challenges of biometrics; including social, ethical, data, and organizational risks and provides several use cases as examples. These risks and challenges lead to **10 key questions**, presented in section three, that programs are urged to consider – and which make up the key guidance to support programs to work through. Section four provides a summary of next steps in implementation, while section five concludes with an overview of research priorities and where to go for more information.

SECTION I

Background

What are biometrics?

Biometric technologies use measurable physical characteristics (fingerprints, facial images, iris scans, etc.) to recognise an individual's uniqueness, or verify his or her claimed identity (4). They can be thought of as technologies of 'capture and comparison': that is, technology is used to capture digital representations of an individual's characteristics, which can be compared over time for recognition (10, 11). Biometric technologies serve two important functions – they can demonstrate that a person is a unique individual to avoid duplication during enrolment ('**identification**'), and that the same person is interacting with a system at each contact (referred to as both '**authentication**' or '**verification**').

What they can't do is establish any of the other information that is required to create an identity record – your name, where you are from, who your parents are, your nationality, etc. As such, biometrics can act as digital tools to enhance identity management systems but are not enough in their own right to establish a legal identity (such as is created when a child has their birth registered).

Biometric 'traits'

The features used to identify individuals are commonly referred to as 'traits' in biometrics. There are three main types of biometric traits used: physical, behavioural and psychological, although the latter two are technologically less well-developed and more suited to use as a secondary confirmation in systems requiring high-end security, rather than the use cases most relevant to UNICEF. As such this guidance focuses on **physical traits**.

A 'good' biometric trait should be **unique and permanent**: it should provide enough information to distinguish individuals from each other over time (2, 12, 13). These, along with five other characteristics, are commonly used to determine the suitability of a biometric trait for a particular use (Box 1).

BOX 1. CHARACTERISTICS OF GOOD BIOMETRIC TRAITS

1. **Unique/distinct**. The ability to adequately discriminate between individuals of an entire population based on the particular trait.
2. **Permanent**. How persistent an individual's biometric trait is over time.
3. **Universal**. Every individual, in general or only those who need access to a certain application or service, should possess the trait.
4. **Measurable**. The system should be able to acquire and digitize the trait without undue inconvenience to the user. The raw data captured must allow for further processing, such as feature extraction.
5. **Performance**. Recognition accuracy in terms of resources required and the constraints imposed by the application.
6. **User acceptance**. The willingness of users to present their trait to the system.
7. **Circumvention**. The difficulty that a trait can be imitated, or obscured (for example, using a silicon finger or wearing a hat to hide facial features).

Source: adapted from Jain et al 2017 (6); Kotzerke 2016 (14); van Greunen 2016 (12)

Traits with the longest history of success in practical applications among adults include facial, fingerprint, palmprint and iris recognition (2). The technology is much less reliable for use with children (particularly very young children). Currently (as of mid-2019), there are no biometric technologies capable of consistently providing high levels of accuracy in very young children (less than five years) (15-17), although several are in development (18-20). Evidence is also weak for use of biometrics in children aged 5–15 years, however the development industry has broadly adopted their use with this age group, including UNHCR and WFP (21, 22), along with several countries as part of national identification systems (8, 23).

Facial recognition is one of the more technologically-challenging biometric traits, as the system must firstly confirm the presence of a face, and then locate the boundaries of it from the space around it (10, 24). New methods in facial recognition have dramatically increased recognition accuracy over the past five years, with more systems able to successfully recognise even poor-quality images (25). As such, facial recognition is quickly becoming the default technology of choice for biometrics systems for use with adults.

Fingerprint recognition is one of the most widespread biometric technologies in use today. Fingertips have distinctive features known as friction ridges, which leave a unique fingerprint. Friction ridges include bifurcations (where a single ridge splits in two) and terminations (where a ridge ends), and their location and direction (called minutiae) allow a fingerprint to be uniquely recognised (10, 24). Like fingerprints, the details of a **palm** can be matched through correlation, mapping the location and direction of ridge points, or ridge pattern markings (26).

Iris recognition uses the unique features of the iris (most commonly, both irises), including rings, furrows, freckles and the corona (27). Among adults, iris recognition is considered one of the most accurate and inclusive biometric technologies, with lower rates of false accepts and rejects (28, 29).

Additional technologies under development include the following:

- **Earprint** recognition uses specifically aligned and normalised photos of the ear to generate measurements relating to unique identifiers of the shape of the outside ridge of the ear (26).
- **Footprint** recognition focuses on characteristics such as length, shape and area of the silhouette curve, local foot widths, lengths of toes, and angles of inter-toe valleys. Soleprint feature extraction extracts the texture-based information of the sole of the foot and minutiae-based ballprint features (30).
- **Hand geometry**. Various measurements on the length, width, thickness, and surface area of the hand and fingers are used to produce a three-dimensional view of the hand (10, 26).
- **Vein pattern** uses near-infrared light to obtain thermal information and map the pattern of veins under the skin, usually applied to the hand or fingertips (24).

When more than one biometric trait is used in combination, it is referred to as '**multi-modal**' biometrics. As well as increasing the number of people likely to be successfully enrolled in a system (31), recognition accuracy is greatly improved with a multi-modal approach (32).[1] The most commonly used and understood form of multi-modal biometrics is the use of multiple traits (such as fingerprints and an iris scan) (33). However, using multiple images of the same trait, or increasing the number of traits enrolled (for example, using all fingers rather than just one) are also forms of multi-modal biometrics (32), and similarly increase recognition accuracy, given the increased amount of data being collected.

1. One study, for example, improved authentication accuracy from 26 to 100 per cent by combining facial recognition with all 10 fingerprints and an iris scan (29)
2. DNA is also not always unique. Twins for example, share the same genetics (and as such, DNA), and so could not be identified from each other in a biometric system using DNA

© UNICEF/UN0155835/Zammit

BOX 2. BIOMETRICS AND DNA

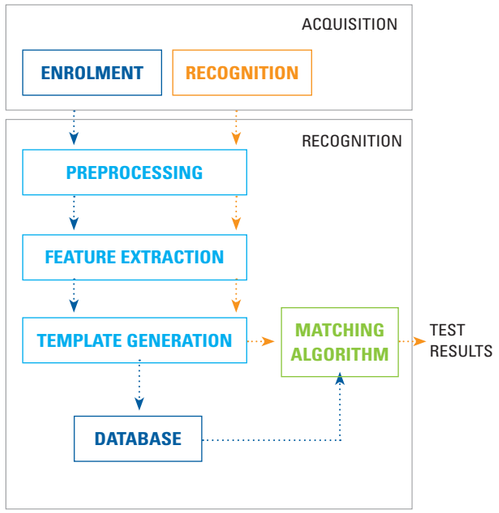
The use of **DNA** in biometric recognition systems deserves special mention. It is the only trait that does not change over an individual's lifetime (10) and so opens the possibility for newborns to be definitively linked to their primary source of legal identity (their birth certificate) from birth (1).[1] While originally a costly process, taking several weeks to process and read the genetic sequence for use in identification; new developments using much shorter sequences of DNA only take around one hour to process, and it is likely this time (and cost) will continue to decrease as the technology advances (1, 4, 28).

However, there are inherent ethical concerns over the level of intrusiveness of using DNA in identification and we therefore **do not recommend the use of this technology** in programs supported through UNICEF as the risks are difficult to fully manage. It is possible to learn much more than someone's identity through their DNA. Sex, medical history (and future health risks), and family relationships, for example, are all 'stored' in our DNA (4). As well as making it much more intrusive from a privacy perspective, this also increases the possibility of increased discrimination against people seeking to access services, especially if datasets become linked (34).

How biometric technology works

There are three important steps in any biometric system (Figure 1): enrolment, template generation, and matching.

FIGURE 1. **SIMPLIFIED PROCESSES WITHIN A BIOMETRIC SYSTEM**



Source: adapted from Du E, 2013 (24)

Enrolment

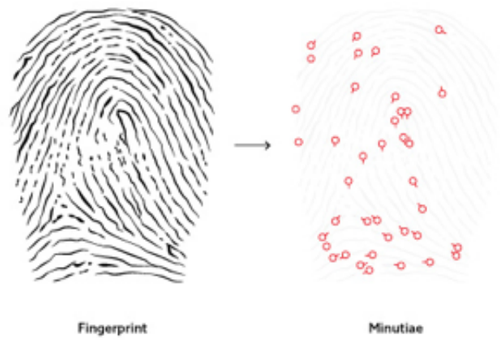
Enrolment involves a user presenting their biometric trait to a sensor in a standardised way to minimise variation (such as the correct amount of pressure for a fingerprint, or a neutral facial expression) (2). The biometric images produced during enrolment are referred to as gallery, reference, stored, or enrolment images. Images presented during recognition are referred to as probe, query, or input images (5). The quality of images captured during enrolment is a key factor in overall performance: images captured with low contrast and/or distortion, and are otherwise of poor quality,[3] generally cannot be improved later on in the process (35).

Template generation

A **template** is not a whole image, but rather a digital code that represents a simplified pattern of the original (Figure 2). During this phase in the process, raw data is processed to identify unique and distinct features; background '**noise**'[4] is reduced or eliminated; and the final images are normalised and saved as standardised digital templates (24). Often, the extracted features (such as the miniate points of a fingerprint) are saved while the raw data (the actual image of the fingertip) is discarded (5).

The process of template generation is very vendor-specific, with each vendor using a variety of different approaches, and limited industry consensus on what common features should be included in a standard template (25). This means that templates created by different systems often cannot be directly compared. If, for example, two organisations wanted to share their biometric systems or create a common platform, they would need to either both use the same proprietary software or must share the original images and create their own biometric templates.[5]

FIGURE 2. **EXAMPLE OF A BIOMETRIC TEMPLATE (BASED ON FINGERPRINT MINUTIAE)**



Source: adapted from Jain, Ross & Nandakumar, 2011 (5)

3. The poor quality of images may be due to the poor quality of the trait itself, such as fingerprints that have been damaged
4. Biometric recognition systems rely on digital measurements of body characteristics, rather than the actual physical traits themselves, and this process of measurement introduces variations, referred to as 'noise'
5. Noting that for some biometric traits, such as fingerprints, standardized compression algorithms have been developed to facilitate data exchange between systems

Matching

The comparison (or matching) of two templates is the most vendor-dependent part of the process and depends on the **matching algorithm**[6] applied and **threshold**[7] level set (33, 35). There are two main types of template matching:

1. During identification, the query template is compared with the biometric template(s) belonging to everyone already in the system. This is usually done to demonstrate the uniqueness of an individual when they are enrolled in a system (to ensure 'de-duplication') and is also referred to as 1:N (one-to-many) matching (1, 4).
2. For authentication, biometric templates are just compared to those already associated with that individual and their template(s). This type of matching is done to confirm they are the same person as was in contact with the system before, and is also called 'verification', or 1:1 (one-to-one) matching (10).

Biometric systems can be automated or semi-automated. In semi-automated systems, the top matches are provided, and an expert manually selects from them (through a process of adjudication). In fully automated systems the system returns all those templates whose match scores exceed a defined threshold (5).

System performance

As with any technology, biometric systems have their limits. In this instance, the process of creating a template (a simplified version of the biometric trait), introduces the potential for errors or 'over-simplification', which can reduce accuracy. Further, as biometric technologies are based on matching thresholds, there must be provisions in place to ensure that false negatives or 'rejections' from the system do not exclude children from essential services.

While knowledge-based identification systems (such as a password or PIN) always accept the correct password, biometric systems are based on a recognition threshold and are therefore never 100 per cent accurate (36). There are a range of issues that can affect system performance (how well this matching works), especially when in identification mode, when the system is being asked to find a match against many records rather than simply matching against a single template as done with authentication (1). Factors that can affect system performance include:

- The quality of the sensor (for example, camera resolution and clarity).
- The interaction of the user with the sensor (eg. how hard they press to take a fingerprint or where the finger is placed on the sensor (33), or whether they keep a neutral expression for facial recognition).
- The quality of the image captured during enrolment.
- The underlying algorithm and complexity of the template (eg. how 'simplified' the digital representation is and therefore the level of detail available for matching).
- The matching threshold programmed into the software (3). It is to be expected that any system will generate some level of 'false rejections' where an individual's template is not recognised by the system even though they have been previously enrolled (2).

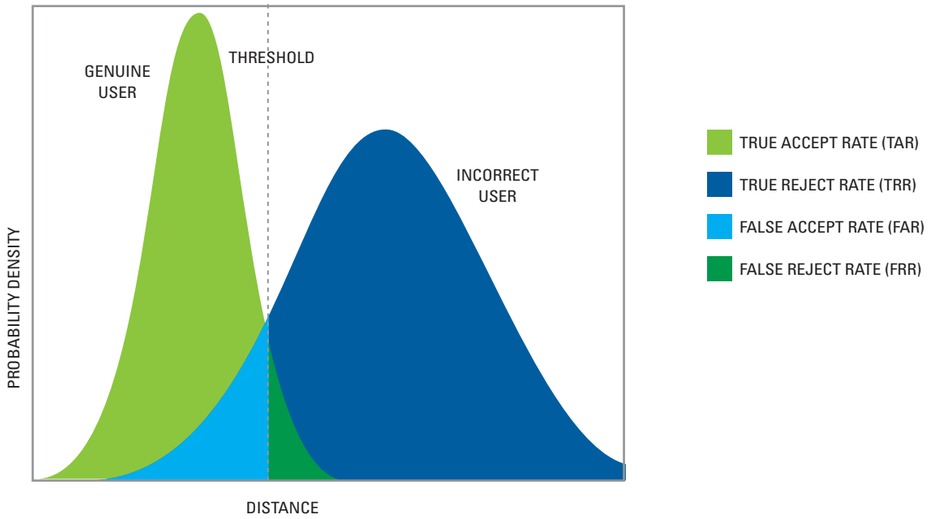
6. An algorithm is a set of mathematical instructions or rules that, especially if given to a computer, will help to calculate an answer to a problem (https://dictionary.cambridge.org/dictionary/english/algorithm)
7. The threshold is the level at which a user's identity will be accepted or rejected. It can be changed – for example, a very secure system (such as passport control) would have a high threshold, with higher rates of false rejections (but lower rates of false accepts)

- The implementation environment: including the impact of heat, humidity or rain on sensors; or the limitations of implementing a fingerprint-based system in a busy factory (where workers are more likely to have worn or damaged fingertips).
- The electrical environment of the country or region, including the need for a clean and stable power supply, and the likelihood of power cuts or surges.
- The broader information technology environment of the country or region, including Internet coverage and reliability, and the ability of local systems to deal with data corruption or viruses, and software crashes.
- The potential impact on users, such as time for recognition (12 seconds versus three minutes), especially for systems that will be implemented in busy settings, or where there are likely to be peaks in demand during the day or week.
- Characteristics such as user age, gender (29),[8] ethnicity (37),[9] disability (38), or occupation (5).

All these factors result in some variation of the templates produced by the same person using the same system. As such, all systems require a **threshold** to be set that determines at what level a user's identity will be accepted or rejected (Figure 3). This threshold reflects a trade-off between the effectiveness of the system for practical application, and the risk of incorrect recognition (3). When variation is too great, and depending on what level the threshold is set at, this can result in a genuine user being rejected from the system ('false negative') or being incorrectly matched with the wrong template (and therefore identified incorrectly) ('false positive') (1, 5, 10).

Recognition errors can be divided into two groups for authentication and identification, as summarised in Table 1.

FIGURE 3. **EXAMPLE 'DECISION LANDSCAPE' SHOWING THE IMPACT THRESHOLD LEVELS HAVE ON RECOGNITION ACCURACY**



Source: adapted from de Luis-Garcia et al, 2003 (33)

8. The 2018 Iris evaluation published by NIST examined accuracy by sex, race and eye colour, and found significant but inconsistent differences in accuracy across different algorithms
9. Recent research for example, has shown substantial disparities in the accuracy of facial recognition systems based on gender and ethnicity

TABLE 1. **SUMMARY TABLE OF COMMON PERFORMANCE METRICS**

		CORRECT USER	INCORRECT USER
AUTHENTICATION	**System accept**	**True accept rate (TAR)** Proportion of genuine users who are correctly matched to their biometric templates	**False accept rate (FAR)** Proportion of users who are incorrectly matched to another user's biometric templates
	System reject	**False reject rate (FRR)** Proportion of genuine users who are incorrectly rejected from the system	**True reject rate (TRR)** Proportion of users who are correctly rejected from the system
		NEW USER	**ENROLLED USER**
IDENTIFICATION	**Identity matched**	**False positive identification rate (FPIR)** Proportion of new users who are incorrectly matched to another user's biometric templates	**Rank-1 Identification** Proportion of enrolled users who are correctly matched to their biometric templates
	Identity not matched	**True negative identification rate (TNIR)** Proportion of new users who are correctly not matched with any biometric templates in the system	**False negative identification rate (FNIR)** Proportion of enrolled users who are incorrectly not returned with an existing biometric template

SECTION II

Benefits, risks, and concerns

Potential benefits

Biometric technologies offer several potential opportunities for improved programming in areas of interest to UNICEF including: improved efficiency by better identification of people targeted for assistance, reducing fraud and duplication, and simplifying registration and recognition processes (34). Depending how a project is designed and implemented, it has been argued that the use of biometric technologies can also enhance privacy (36) by limiting the information people need to provide at the point of service, for example, by not having to provide their name in a busy health clinic (1, 39, 40).

However, many of these functions can also be met through good data management procedures and any form of unique identifier (such as a personal identification number), although biometric technologies may greatly simplify the interaction that individuals need to have with the systems providing these services.

Efficiency and continuity of service

Biometric technologies provide new opportunities to leap-frog traditional paper-based systems, improving outreach and enrolment in identity systems and reducing the time required for an individual to demonstrate their identity credentials (1). Biometrics offer the advantage of not relying on biographic identifiers such as names, which are shared by many people and can be spelt or used differently pending circumstance; or date of birth, which can be unknown.

Biometric technologies can be a useful tool for linking data together in different systems, especially where routine data systems are weak, and therefore improving continuity of services across sites or sectors (1, 39-41). They may also help with tracking in programs that have a longitudinal data component such as vaccination services (28, 42-44) and tuberculosis treatment monitoring (Box 3), or monitoring school attendance to better understand children at risk of 'dropping out' (Box 4).

BOX 3. BIOMETRICS AND HEALTHCARE

Several countries in Africa have implemented a biometric fingerprint recognition system (VaxTrac), which takes fingerprints from both the child and mother of the child to accurately verify the identity of the child and determine what, if any, vaccinations have already been administered (18).

Operation ASHA in India has implemented a fingerprint recognition system that takes prints from both the patient and employee in tuberculosis treatment clinics (18, 28). Once registered, patient data is sent to a central server at the end of each day and clinicians receive text messages if a patient has missed an appointment, with early results showing improved outcomes for patients enrolled in the biometric system. In Kenya, USAID has piloted a similar biometrics system to help track youth health, particularly focussing on HIV. The system was implemented to guard against double-enrolment and help with tracking youths across multiple providers (45).

BOX 4. BIOMETRICS AND EDUCATION

Schools in a range of countries (including India, Nigeria, Pakistan, the United Kingdom and USA) are implementing biometric systems for recording staff and student attendance and improving security over physical access to buildings (1, 46, 47). One such example is in Kenya where the Ministry of Education, Science and Technology (along with Save the Children) has implemented an iris-based authentication system to track student attendance. The system aims to provide an accurate attendance mechanism for all students with text messages sent to parents in real-time if their child is late or absent (46).

Biometrics have also been used in the education sector in Nigeria to help prevent exam fraud by enrolling students during their regular classes, and then requiring their biometric for identification at exams (1).

Reducing fraud

A common reason for the use of biometrics is to enhance the accuracy and integrity of development interventions by reducing fraud (48). UNHCR introduced their official policy on biometric registration systems in 2010 (49), and in 2012, UNHCR Jordan introduced iris-scanning biometric authentication into its cash assistance program to reduce the risk of fraud and ensure money reaches the intended recipients (21). UN partners – including UNHCR, WFP and IOM now routinely use biometrics across their cash programming and other programs to ensure resources reach those they are meant to.

Reducing fraud has also been a key driver of government identification systems based on biometrics – such as India's Aadhaar system (50, 51). Biometrics, primarily fingerprints and iris, have been used to create beneficiary registries and authenticate cash or in-kind transfers, usually combined with electronic payment, in at least 15 countries including Afghanistan, Bolivia, Botswana, Democratic Republic of Congo, Ghana, India, Indonesia, Iraq, Kenya, Malawi, Namibia, Nigeria, Pakistan, the Philippines, and South Africa (52).

UNICEF is most likely to consider the use of biometrics to reduce fraud through the integration of biometrics into the Cash Transfers Management Information System currently under development for our cash programming in humanitarian settings or in collaboration with third party systems that work with us to manage cash payments and transfers. More broadly, we are also likely to be asked to work with government and other partners looking to include biometrics in national or service delivery management systems in sectors such as social welfare, education and child protection.

Enrolment and recognition

The use of biometrics, in combination with other technologies, is being used to register, deduplicate and enrol undocumented immigrants and refugees (21), and may provide an additional tool for countries that lack effective identification systems by using patterns of contact with government or agency services to establish a recognised identity (53).[10] In these instances, individuals and families may be allowed to claim the services and protection they are entitled to but have not been receiving due to a lack of registration and/or documentation. It is also argued that a biometric-based system can simplify interactions with government agencies and minimise the data needed to be shared to validate one's eligibility to access services once a legal identity has been established.

Biometric-based national identification systems, primarily using fingerprints and iris scans, are currently in place in several countries with notable examples including India, Estonia, and large parts of Latin America. Currently, some 15 African nations have implemented national biometric ID systems, with the minimum age of enrolment between 15 and 16 years old, and primarily using fingerprint and facial recognition (8). It should be noted that the UN has established a multi-agency approach to ensure a 'life-cycle' approach to legal identity and ensure that these biometric systems are linked to civil registration (Box 5) – ensuring that legal identity is established at birth and 'retired' at death – regardless of whether or at what age a biometric may be applied.

10. This approach to building an identity through a 'tracked history', while important for those without legal identification, is not a replacement for legal identification being established through birth registration and tends to exclude children from these opportunities

BOX 5. BIOMETRICS AND IDENTITY: UNDERSTANDING WHAT BIOMETRIC TECHNOLOGIES CAN AND CANNOT DO

It is important to make the distinction between biometric technology as a tool for recognition; and the legal identity of an individual, which establishes the identity of an individual by the State and is a universal human right. Birth registration, as part of an effective civil registration and vital statistics (CRVS) system, is the gold standard in establishing a legal identity: the foundation of human rights protections, and captured under the Universal Declaration of Human Rights and the Convention on the Rights of the Child (CRC) (4). For children, a birth certificate is often the only form of legal identity. Without proof of legal identity, people often face barriers to accessing services, including education, employment, social transfers, financial services, and voting (28).

As noted previously – biometric technology can be used to **demonstrate the uniqueness of an individual** when they are enrolled by comparing their biometrics against those already in the system (1). Much like a PIN or password, they can also be used to **authenticate (or validate) that an individual is entitled to access a system or service** (10). Biometrics can enable access to various systems and uniquely identify an individual, however biometrics alone are unable to confirm the legal identity of an individual and are limited in uses – as they can only authenticate that the biometrics provided match the data captured in the system (34). Biometric systems can therefore support legal or functional identity systems,[11] but are not in themselves a substitute for the lack of essential documents like birth certificates.

Much of the biometric literature has strongly argued that biometric technologies are an effective means of providing a unique identity from birth (6), providing immediate identity security for newborns to help prevent cases of mistaken identity, illegal adoption, and abduction (14, 17, 54-56). However, this would require routine enrolment of all infants from birth. Currently this is only possibly through DNA, so not recommended by UNICEF.[12]

Biometrics are also referred to as a potential means to prevent child trafficking, by providing efficient means of recognition at border crossings, hospitals, airports and bus stations (15, 54). Anecdotal reports have shared incidences where children have turned up in refugee or displaced camp settings for enrolment with a different name, set of details and family, but their biometrics have linked to a previously enrolled child – indicating that the child may have been trafficked (Box 6).

BOX 6. BIOMETRICS AND CHILD PROTECTION

Since its establishment in 1997, over 26 million fingerprint kits have been distributed to families as part of the USA's National Child ID Program, allowing parents to take a fingerprint of their child (which they retain), to assist with recognition in cases of abduction or missing persons. No data has been released on performance (18). In South Korea, fingerprints and photos of over 3.5 million children under the age of 18 years have been stored on a government database, developed in part to help authorities locate missing and abducted children, particularly those with mental disabilities and dementia (57).

Several countries are proposing biometric technologies to strengthen child protection, including China, which would have parents take their children to registration centres to have their iris scanned. If a child who is registered on the database goes missing and is found, an iris scan will be able to determine his or her identity (58).

Risks of using biometric technologies

There are a range of risks that should be considered when evaluating whether the potential harm from a proposed biometric system is adequately managed and outweighed by the possible benefits as described above. A key difference with biometric technology in comparison with other digital technologies is that it has the **potential for harm that cannot be fixed or adjusted** (34). Various social and ethical risks have been highlighted. These, along with data and organizational risks (13) are discussed in detail below.

Exclusion and coercion

One of the biggest concerns regarding biometric technologies is the risk of exclusion. When actual system failures occur such as a failure to enrol, or a false rejection, it raises the risk of exclusion as the burden of proof (that is, proving the system is at fault) tends to fall on the individual in question. The potential for exclusion is made worse by the likelihood that these failures or errors are more likely to occur in children, and others who may be from disadvantaged groups such as manual labourers, those affected by disability, or the elderly (1, 14). Algorithms may also have inherent biases built in, which mean they are better at recognising some people than others (based on age, gender, skin colour, etc.) (48, 59). Recent research from the National Institute of Standards and Technology (NIST), for example, showed significant differences in accuracy between males and females in some of the latest iris-recognition systems (29); and a study on facial recognition showed 'substantial disparities in the accuracy' of systems between males and females, and between darker- and lighter-skinned people (37).

11. Noting that most biometric technologies are not suitable for use with young children at present
12. The risks associated with universal collection of a biometric at birth are significant –in terms of data privacy and protection, as well as from erroneous enrolment or errors that would have lifelong impacts and would be difficult to undo, and the potential for later problems from potential mismatches to the identity record if the biometric used does not 'age' in the manner predicted by the algorithm – resulting in difficulties matching a later 'query' template to the original enrolment template

The impact of being excluded from services is not insignificant. In 2013, over 6,500 refugees in the Mbera camp in Mauritania were denied access to refugee assistance due to problems with the biometric registration system (52). Similar issues were noted in performance data of India's Aadhaar system during roll-out in 2012 (1), more recently in Rajasthan (50), and an investigation into the 10 reported hunger-related child deaths between 2015 and 2018 showed many of the families had either lost their Aadhaar-linked ration card, or were not able to enrol in the system (60). Overall, it is important that all biometric systems have a 'fail-safe' to ensure that essential services are not denied in the event of system failures or errors.

Biometrics may also restrict access to services as it is difficult to provide comprehensive coverage when people cannot or do not want to enrol in the system established to support that provision. This may occur when parts of the population withdraw due to potentially exclusionary policies (12, 28), when children who should benefit from the service are unable to have their biometric trait captured, or when parents do not wish to have their child enrolled in a biometric system (40). One of the key concerns raised against the biometric system used in Pakistan after the 2010 floods related to grievance resolution processes in the case of wrongful exclusion from services (28).

This linking of access to services with the provision of biometric data, especially where there are low levels of user acceptance, also raises issues around coercion. While Aadhaar is not mandatory, it now includes a comprehensive network of banks, government services, shops, and point-of-service facilities (61): as such, the 'voluntary' nature of the system has been called into question (50, 52). Given the asymmetric power relationship between individuals and humanitarian organisations (and governments – see Box 7), there are concerns over the ability of vulnerable groups to voice their discomfort or opposition to biometric technologies (34, 49), an example being the Eurodac system, which has by default become a 'a de facto prerequisite to claiming asylum' (52).

BOX 7. BIOMETRICS AND COERCION

The 'physicals for all' health program implemented in Xinjiang province, China, which collects DNA samples along with iris scans of all citizens aged 12 to 65 years, was flagged by Human Rights Watch as a potential means of surveillance, with individuals not given the choice to participate, and DNA samples to be provided at the same time as renewal applications for household registration documents (62).

Data risks

The characteristics that make biometrics an optimal basis for identification, their uniqueness and permanence, also make their data processing of particular concern, as once replicated and stored, individuals are no longer the sole possessor of their own biometric data (34, 63). This can lead to data misuse in terms of potential future applications, both known and unknown, and also data misuse in terms of theft or abuse (40). Biometrics inherently enhance the ability of systems to share, track and link data, and therefore must also address the broader concerns of addressing privacy and protection as data becomes more accessible to new users and stored in more places.

Data protection and privacy

While the number of developing countries with data protection or privacy laws is increasing, many still have weak rule of law, with limited accountability or authority for implementation (28, 40). This is of concern for biometric systems, given the richness of information that biometrics provide, which have much greater consequences when misused, abused, lost or stolen. While biometrics do facilitate more immediate traceability of aid delivery, for example, this improved traceability also creates additional privacy risks, including granular data about the movements of vulnerable individuals, allowing for precise and private inferences to be made about their lives (34). This can lead to serious consequences when governments of host countries or those from refugee's countries of origin request or demand humanitarian data, to repurpose for law enforcement of national security screening (7).

Scope creep

Biometric systems, along with digital identification systems more generally, increase the risk of scope creep, that is, when data is used for new purposes or shared with others who use it for purposes outside of the scope of original collection, and for which informed consent has not been given (64). This can happen when the aims of the collecting organization change over time, or when data are shared with other organizations that have different aims or are less worried about who they also share the data with (40). Scope creep is more likely to occur if more data is collected than what is needed and kept for longer retention periods than required.

It has been documented as a 'profound' issue including: India's Aadhaar system, which has become a mandatory pre-requisite for access to many services including private banking (61); the amendment to Eurodac in 2015 allowing law enforcement authorities to conduct 'targeted fingerprint searches' in connection with certain serious crimes and terrorism offences (3, 65);[13] and plans to link fingerprint data with closed-circuit television in Mexico to verify that beneficiaries are complying with healthcare requirements (1).

Data ownership

Biometric data can also be sold, with or without the explicit knowledge of the individuals it belongs to (9, 66, 67). For example, it is common practice for researchers to acquire biometric data from vendors to enhance their database gallery size when conducting identification tests (6). Data can also be shared between partners with different levels of data protection in place.

Organizational risks

There are important legal, operational and reputational risks for humanitarian agencies when collecting and holding vast amounts of biometric data, and this leads to issues around both actual and perceived risks (34). Actual risks are just that: a data breach or security threat whereby the biometric data of beneficiaries are stolen or corrupted or requested by a government agency. Perceived risks relate to the potential for misinformation to erode the trust beneficiaries place in UNICEF and its partners around the use and need of biometric data as part of its programs.

The general principles of good data management as adopted by the UN system should be employed to all data systems including those that incorporate biometrics.[14] The OECD's data privacy principles are also relevant.[15]

13. Outside the scope of Eurodac's initial purpose: to help assign the country responsible for processing claims of asylum
14. Available at: https://www.unsceb.org/principles-personal-data-protection-and-privacy
15. Available at: http://oecdprivacy.org/

Specific risks for children

Biometric technologies also pose specific risks for children, including data protection and privacy, exclusion through system design or technology limitations and failures, and unintended uses of linked data. As well as the general risks that apply when implementing any digital identity management system, specific consideration should be given the potential impact on children for three important reasons:

1. Biometric systems have primarily been designed to work with adults, and as such, the **technology is not always appropriate** for use in recognizing children. This may be due to the difficulty in capturing the biometric trait (such as an iris scan with very young children); the relatively poor performance of the trait among certain age groups (facial recognition); or the low levels of user acceptance (DNA).
2. Children are more vulnerable than adults, and this creates additional **social and ethical risks** than when working with the adult population. Children often lack the agency or opportunity to be involved in making important decisions about their participation in certain services and programs. They also lack the knowledge and understanding required to make informed decisions about the processing of their own personal data, including the risks and consequences (9). While requiring parental consent is an important means of addressing such issues, many parents or guardians may also not fully understand the risks either, thus increasing the vulnerability of children (68).
3. Children are at the forefront of the 'big data' revolution, and this increases their likelihood of being exposed to **lifelong data risks**, including privacy and security concerns. With the rapid development of technologies for the collection and analysis of data, more data will be collected on children over their lifetime than ever before, and the future use, applications and impact of this data on their lives is unpredictable (9).

Overall, the misuse of children's biometric information can have permanent and serious consequences, especially in terms of privacy and identity fraud. While biometric technologies have the potential to strengthen identity management systems; they also have the potential to disrupt and lock-in the identities of children from a much earlier age (28).

SECTION III

Practical approaches in assessing the use of biometric technologies

How to use this guidance

This section provides practical guidance and associated tools for assessing whether it makes sense to consider moving ahead with implementing or supporting biometric technology in specific circumstances, by working through the balance of benefits and risks, and whether those risks can be safely managed.

In order to use these tools – it is recommended that programs first complete the brief project outline provided in Annex 1, which collates basic information on what you propose to do, and which will be needed to work through the following questions. A series of **10 questions** is then presented for consideration – summarised in the flowchart (next page) and explained in more detail on the following pages. Each of these questions will provide a basic indication of whether you should stop and reconsider your proposal, whether you need to exercise caution and work through some potential risks to make sure they are properly managed before proceeding, or whether it is safe to move onto the following question. While each question can be dealt with in any order, they have been ordered in the manner presented as we feel this is the most logical way of working through them against the information you will have started to collate in Annex 1 (and which you will want to update as you go).

At the end of this process you should have reached one of three outcomes:

1. If you have reached a recommendation to **STOP** – there is strong reason to re-think the need to include biometrics and to look at redesigning your approach. Please do consider reaching out to the Data Help Desk (see contact details at the end of this document) to talk through the project if you need additional support to discuss alternatives or understand why this approach is not recommended.
2. If you are working through questions for which the guidance has advised **CAUTION** ⚠ – you may need to seek additional information from vendors and experts to determine if your project should proceed. Again – please reach out to the Innovation team and/or Data Help Desk so that we can assist in linking you with the appropriate information. We will also be building out additional guidance and tools over the next year to help work through these questions.
3. If you have reached the end of the ten questions and have addressed the key issues raised – there is reason to believe that biometrics would add value to the program design, and you will now need to work through design and implementation issues. A short overview of things to consider at the implementation stage is given in Section IV, with additional tools to be built as we move forward. It is recommended that you engage with your regional T4D advisor and/or the Innovation team (see the contacts section) to support this stage of the process. If you have updated the form in Annex 1 as you worked through the questions – you should also now have a brief two-page project description that you can use to engage others in the organisation to help you move forward.

FLOWCHART - KEY QUESTIONS

LEGEND | YES | NO | UNSURE | REVIEW | CAUTION | STOP | FOR MORE INFORMATION CONTACT

START

DEFINE THE PROGRAM, OBJECTIVES AND AGE GROUPS

1. VALUE ADD

1.1 Is a unique identifier required to identify people accessing or enrolling in the service or program?
- NO / UNSURE → This is a limited use case for biometrics → Data Help Desk; Office of Innovation
- YES →

1.2 Does using a biometric identifier have strong advantages in this context over other identification approaches (such as a PIN)?
- NO / UNSURE → The use of biometrics is probably not justified → Data Help Desk; Office of Innovation
- YES →

2. LEGAL BASIS

2.1 Is enrolment in the biometric system optional?
- NO / UNSURE → 2.4 Is there another strong legal justification for using biometrics that is consistent with UNICEF's mandate?
  - NO / UNSURE → While UNICEF may support compulsory enrolment in some biometric programs (government ID linkages), there is some concern here around the protection of rights, especially for children → Data Help Desk; Data Protection and Privacy Specialist
  - YES →
- YES →

2.2 Is informed consent to be obtained?
- NO / UNSURE → 2.4 (as above)
- YES →

2.3 Are there penalties to not enrolling that may be seen as 'coercion'?
- NO / UNSURE → 2.4 (as above)
- YES →

3. APPROPRIATENESS

Review options for suitable biometric traits by age group

3.1 Is the selected biometric trait appropriate for the target age group(s)?
- NO / UNSURE → 3.2 Can the biometric trait be changed to another, more appropriate, option? If not, can the age groups be modified?
  - NO / UNSURE → Your project is likely to have high rates of 'failure to acquire' and/or 'failure to enrol' → Office of Innovation; Regional T4D Advisor
  - YES →
- YES →

4. ACCURACY AND RELIABILITY

Review accuracy of biometric traits by age group and purpose

4.1 Is the selected biometric trait accurate for the proposed project use? Consider: does the system have to perform identification (1:n) matching?
- NO / UNSURE → 4.2 Is the project a pilot of new biometric technology, or has the technology changed considerably in recent years?
  - NO / UNSURE → There is currently no proven technology for your selected age group → Data Help Desk; Office of Innovation; Regional T4D Advisor
  - YES → As with any new technology, a project including biometrics needs to be well-planned in advance
- YES →

4.3 Will the biometric trait be used for recognition over a short term period (1-2 years)?
- NO / UNSURE → 4.4 Can the age groups be re-defined or can the biometric trait be re-acquired at suitable intervals?
  - NO / UNSURE → Biometrics are unlikely to be reliable for the duration of your project or system → Go back and consider a different biometric trait → START
  - YES →
- YES →

4.3 Is the biometric trait likely to be stable in all the target age groups over this period?
- NO / UNSURE → 4.4 (as above)
- YES →

5. IMPLEMENTATION SETTING

5.1 Is the system able to operate effectively in the proposed setting? Consider: environment (dust, humdity), portability of the system (does it need to be transported, waterproof), target population, etc.
- NO / UNSURE → 5.2 Can these issues be adequately addressed through proper planning and risk mitigation strategies?
  - NO / UNSURE → Many projects have failed due to implementation challenges → Office of Innovation; Regional T4D Advisor
  - YES →
- YES →

5.3 Will data (biometric templates) need to be shared over a network for matching?
- NO / UNSURE → 5.4 Does the setting support the use of cloud computing, such as having a good network or internet coverage and reliable power?
  - NO / UNSURE → Automated biometric systems search many templates (especially in identification mode) and require the ability to access central databases with high computational power. Decentralised databases also need to be periodically updated. Without reliable Internet connectivity, the systems will become unreliable
  - YES →
- YES →

6. USER ACCEPTABILITY

6.1 Are there sensitivities in the general community that may impact the acceptability of the biometric trait or reason for data capture?
- NO / UNSURE → 6.3 Can these be dealt with adequately through program design and implementation?
  - NO / UNSURE → If user acceptability is likely to be an issue, make sure there are alternative settings or approaches that could be used as part of community sensitisation or enrolment → Regional C4D team
  - YES →
- YES →

6.2 Are there specific groups within the community that may have additional acceptability concerns?
- NO / UNSURE → 6.3 (as above)
- YES →

7. EXCLUSION

7.1 Are there specific groups that may be excluded or specifically concered because of the use of biometrics?
- NO / UNSURE → If the biometric program creates concern for specific groups (ie. women/children), either due to the biometric trait itself or the data collected alongside and as part of the program, risks versus benefits must be assessed and mitigation strategies considered if moving ahead → 7.3 Can sensitivities be managed without excluding children from services or impinging on their rights?
  - NO / UNSURE → Biometric technologies are not recommended → Data Help Desk
  - YES →
- YES →

7.2 Is there potential for exclusion due to physical location, demographics, disability, ethnicity, citizenship status, etc.?
- NO / UNSURE → If the biometric program creates concern for specific groups (ie. women/children), either due to the biometric trait itself or the data collected alongside and as part of the program, risks versus benefits must be assessed and mitigation strategies considered if moving ahead
- YES →

8. DATA PROTECTION

8.1 Is there documentation or processes in place to ensure data associated with the system is protected from external risks and breaches from collection to destruction?
- NO / UNSURE → Review the Good Practice Principles on Information Handling and Management in Child Protection Information Management Systems and document these → Data Help Desk; Data Protection and Privacy Specialist; Regional T4D Advisors
- YES →

9. PRIVACY

9.1 Are the purposes for which the data can be used clearly documented or defined in the consent or legal basis for collection?
- NO / UNSURE → Review the Good Practice Principles on Information Handling and Management in Child Protection Information Management Systems → Data Help Desk; Data Protection and Privacy Specialist; Regional T4D Advisors
- YES →

9.2 Could data potentially be used for different purposes other than those defined in the original collection at a later time?
- NO / UNSURE → Review the Good Practice Principles on Information Handling and Management in Child Protection Information Management Systems
- YES →

9.3 Is access and ownership to data clearly defined and managed in both procedural documents and practice?
- NO / UNSURE → Review the Good Practice Principles on Information Handling and Management in Child Protection Information Management Systems
- YES →

9.4 Are there penalties and procedures for dealing with data breaches and inappropriate use?
- NO / UNSURE → Review the Good Practice Principles on Information Handling and Management in Child Protection Information Management Systems
- YES →

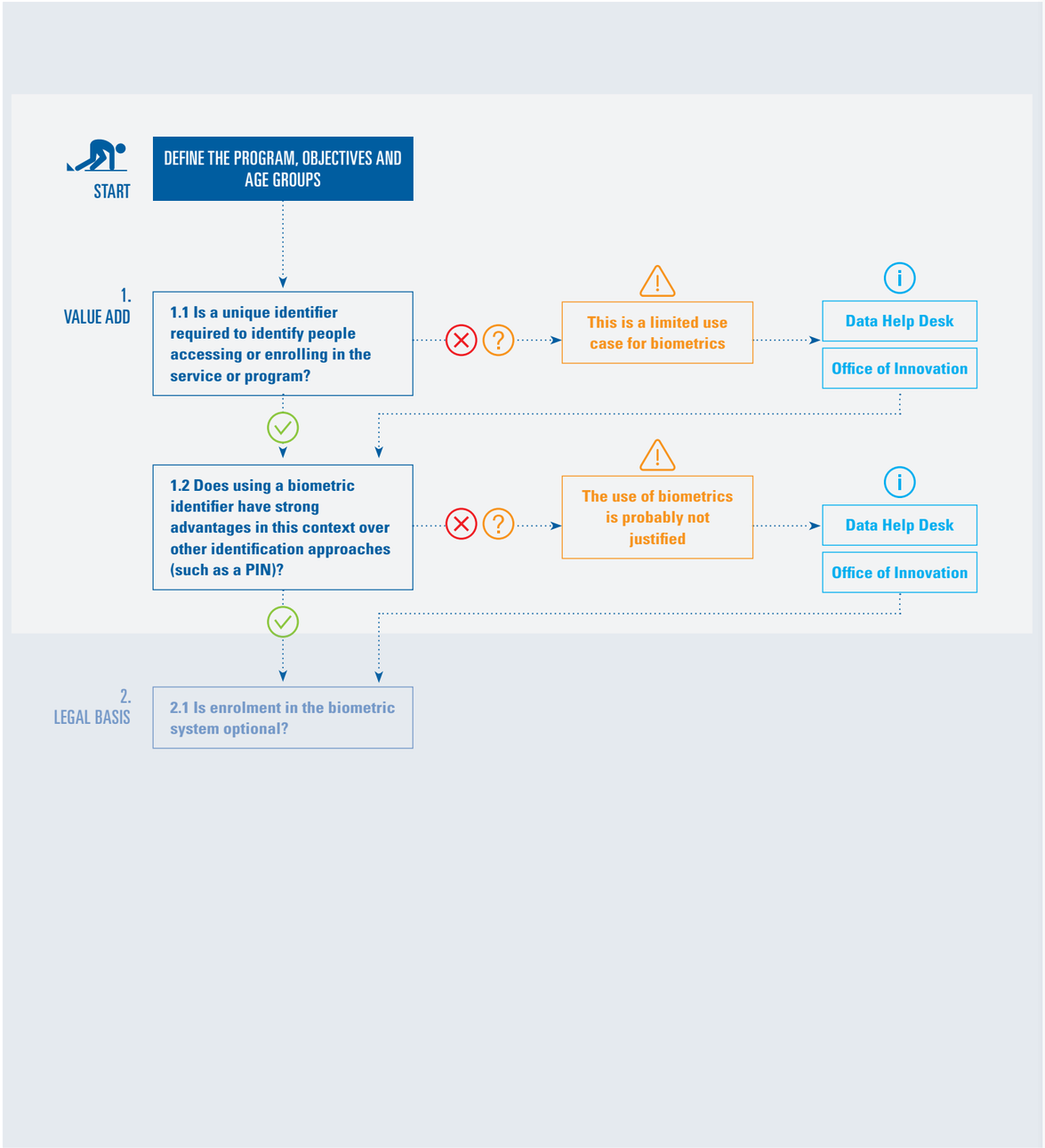
10. PARTNERS

10.1 Does government law require you to share data collected through your program?
- NO / UNSURE → A whole of life-cycle approach to data is important. Data sharing agreements should ensure enforceability → Data Protection and Privacy Specialist
- YES →

10.2 Are all partners (government, UN family, third-party providers, etc.) bound to the same level of data protection and privacy?
- NO / UNSURE → A whole of life-cycle approach to data is important. Data sharing agreements should ensure enforceability
- YES →

BIOMETRICS MAY BE A SUITABLE OPTION FOR YOUR PROJECT OR PROGRAM

END



Q1 Does the use of biometric technology add value to the program?

Due to the risks involved- **the collection of biometric data should directly contribute to better program outcomes than would be possible without this data** (Box 8). That means that the use of a biometric trait should be expected to provide benefits above and beyond the use of other means of identifying individuals; including improved record management, other forms of data collection, and non-biometric unique identifiers such as a personal identification number.

Biometric technologies have the potential to cause harm to individuals when linked with the provision of social services, such as healthcare. In the case of false rejection, when an individual cannot be matched to their enrolled template; there is the risk of exclusion from services. However in the case of false positives, when an incorrect individual is matched to a template and other person's identity, there is the risk of a patient being administered the wrong medication (40). In many applications, biometric systems will need to be integrated with already existing software platforms that use case management tools with searchable identifiers such as names – thus negating most of the added benefit of including biometric data.

Overall, how will the inclusion of biometric technologies add value to your program? Consider the three broad areas of potential benefit:

1. Improved efficiency of continuity of service.
2. Ability to reduce fraud.
3. Ability to **uniquely identify people** accessing or enrolling in the service or program. If there is a need to uniquely identify people, does using a biometric identifier have strong advantages over the use of other means of identification (such as using standard biographic information (name, date of birth, etc.), a PIN, access card, paper-based ID, etc.) (Box 9)? Again, if the answer is no, then the use of biometrics is probably not justified. If the program already uses some form of unique identifier – why is it not working adequately? What are the issues and challenges? How many of these will be resolved through using biometric technologies?

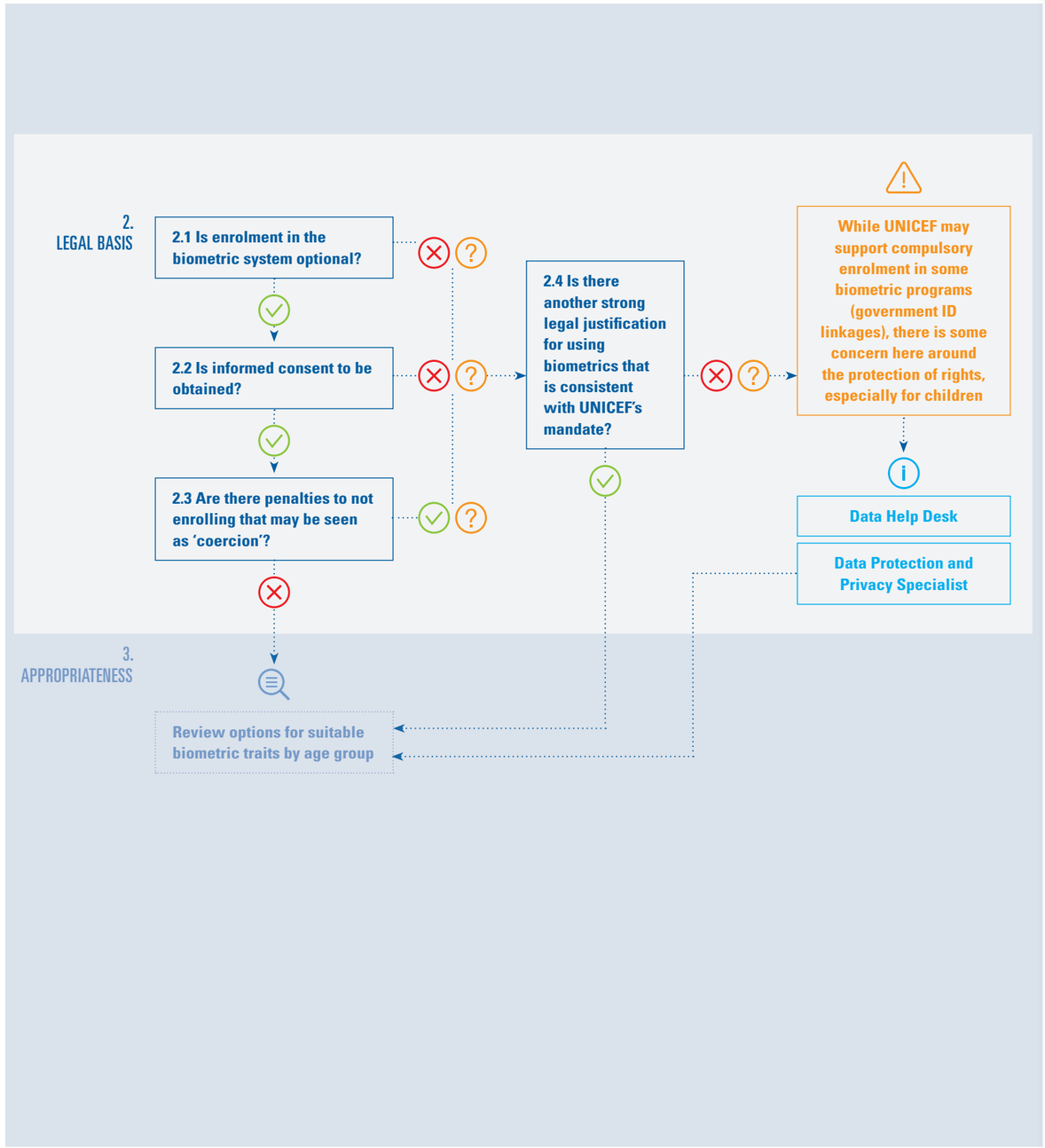
BOX 8. USE OF BIOMETRIC REGISTRATION AND IDENTIFICATION SYSTEMS FOR UNICEF ESAR PROGRAMMING – FINAL GUIDANCE NOTE (JULY 2018)

"In general, the use of third-party registration and identification systems is not recommended for use in contexts where the UNICEF Country Office is largely implementing traditional "development" programming or for use in government-led programmes. This includes, for example, use of existing third-party systems to support or interface with social protection, health management information systems or birth registration systems.

In fragile or conflict-affected environments, however, where a national government-led beneficiary registration or identification system does not exist or in contexts that preclude sharing of beneficiary information with government, third party beneficiary data systems may help UNICEF to improve information management and delivery of services and are in the best interests of those that we support."

Update Q1 in the biometric project planning template

For more information contact the Data Help Desk and Office of Innovation



Q2 Is there an established legal basis for collecting, receiving, or sharing biometric data?

To justify the collection (or receipt from a third party) and transfer of biometric data there needs to be legal grounds.[16] Legal bases provided for in existing international and regional instruments include:

- **Informed consent of the data subject**. Consent is the most popular and often preferred legal basis for processing personal data, including biometrics. This would entail providing enough information to the beneficiaries to ensure transparency and enable them to provide (or decline) informed consent to have their personal data processed. Information notices can be provided to this end, and may cover the following: What is the purpose of the project? What data is being collected? How long will the data be stored? To whom will the data be transferred? What are the rights of the beneficiaries? What are the implications if they decide to withdraw their data? What, if any, are the consequences if they decide not to participate? If beneficiaries are young children, consent may only be obtained through a legal guardian (Box 10).
- **Vital interest** refers to the processing of personal data to protect the life, integrity, health, dignity or security of the data subject or another person.
- **Public interest** of the data subject or of another person. Refers to the processing of personal data as part of the implementation of UNICEF's mandate (as laid out in international conventions).
- **Performance of a contract**.
- **Compliance with a legal obligation**.
- **Legitimate interests of the humanitarian organization**. In this regard, the Handbook on Data Protection in Humanitarian Action,[17] is to be considered. It provides that; 'Humanitarian Organizations may also process Personal Data where this is in their legitimate interest, in particular, when a specific humanitarian activity is listed in their mission, and provided that this interest is not overridden by the fundamental rights and freedoms of the Data Subject. In all of these situations, the term "necessary" is to be strictly construed (ie. the data Processing should be truly necessary, rather than just convenient, to fulfil the relevant purpose)' (71).

BOX 9. ENSURING VALUE-ADD

Several countries in Latin America have implemented national electronic immunization registries (EIR) without biometrics to improve coverage monitoring, timeliness and accuracy. Countries with high levels of birth registration, such as Chile and Costa Rica, have linked their EIR to their CRVS systems, while most other countries rely on registration at the time of vaccination (69).

Despite a number of countries implementing biometric recognition systems to monitor attendance, there is limited evidence to justify the collection of biometric data in education settings, instead of or in addition to, traditional methods (such as through a roll-call, or access card) (70), or other forms of technologies (such as mobile-phone enabled real-time monitoring).

Using biometrics to enhance the accuracy and integrity of development interventions by reducing fraud among beneficiaries (48) only allows for accountability (authentication) checks to be performed at the 'downstream' (point of service) part of the process, largely ignoring 'upstream' factors in the supply chain (34). Further, reducing fraud can also be achieved through other, non-biometric, means. Argentina, for example, was able to save approximately US$100 million in reduced leakage by using a unique identification number across 13 databases including employment, pension, electoral, social, real estate, and automotive records (1).

16. These will be further specified in the upcoming UNICEF global data protection policy
17. Available at: https://www.icrc.org/en/publication/handbook-data-protection-humanitarian-action

BOX 10. CHILDREN AND INFORMED CONSENT

While informed consent provides a legitimate legal basis for the collection or receipt of biometric data, many if not most children under age 13 are **unlikely to have the capacity to provide informed consent** to the processing of their personal data (68). Enabling parental consent to substitute for children's consent may be one way of ensuring children's rights are protected, but given the shortfall in technical literacy for adults, particularly in emerging areas such as biometric technologies, parental consent may be an ineffective way of protecting the privacy rights of young children.

Teenagers and older children often **struggle to understand the implications of providing personal data**, especially the potential long-term consequences. As such, it is important to consider the evolving capacity of children, including age, level of maturity and development, and/or other factors when defining 'informed consent' (72). It is equally important to consider the legal implications of local data privacy laws relating to children's data, such as the General Data Protection Regulation's 'right to be forgotten'.

The requirement of legal basis would cover situations where, for example, the data is:

- collected by government for internal use under the framework of legislation that explicitly addresses who can collect data and how it should be protected,
- collected by UNICEF with informed consent from adults, children or caregivers,
- shared with UNICEF by a third party in the context of a documented data sharing agreement (either local or global) – where the data is required to implement UNICEF's mandate.

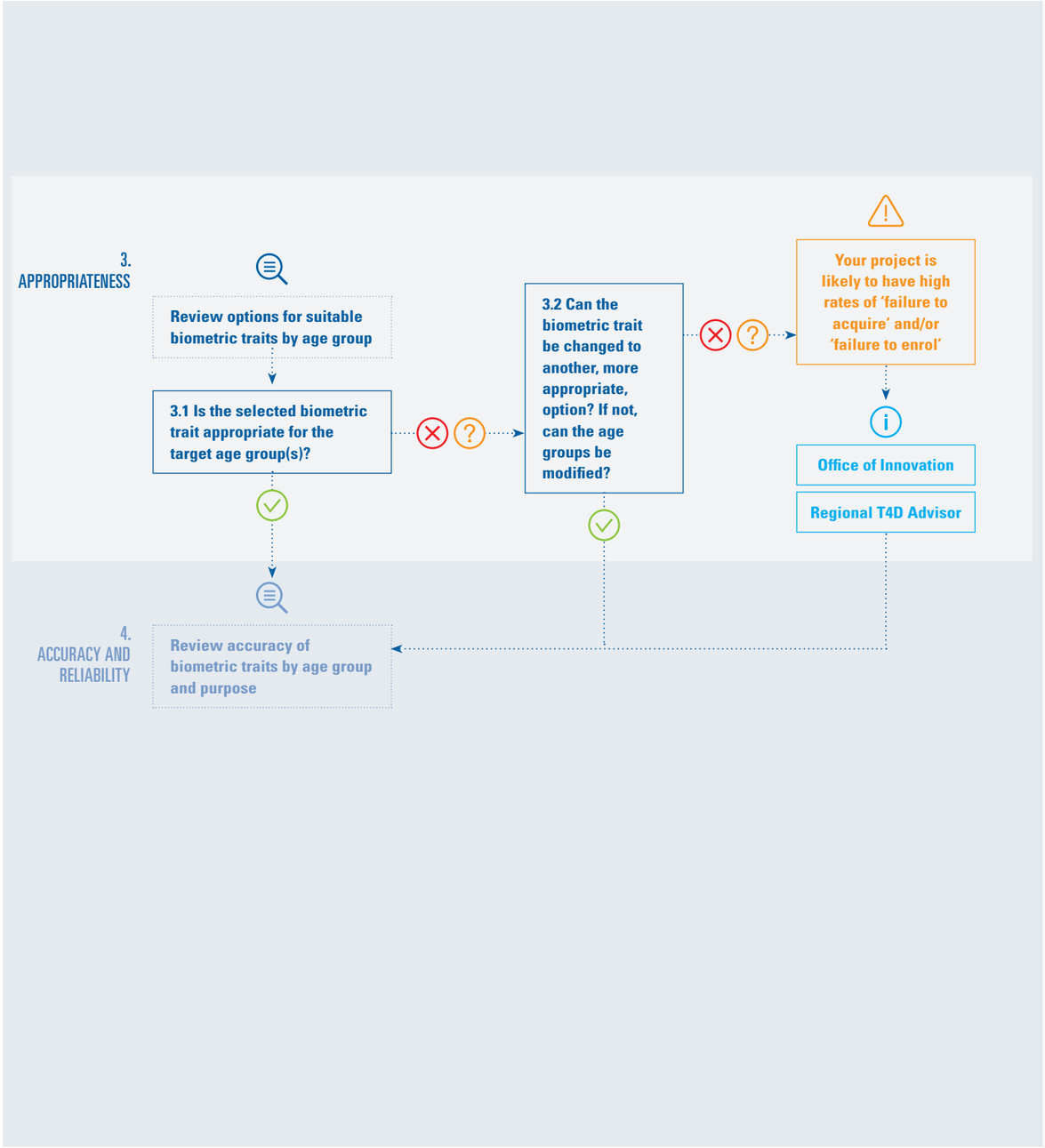
Overall, there must be a lawful purpose for the collection of biometric data. Two important questions to consider: is free and **informed consent**[18] to be obtained, and if so, have disincentives and penalties for not enrolling been avoided? If not, is there another legal justification for using biometrics, consistent with UNICEF's mandate? While UNICEF may support compulsory enrolment in some biometric programs (such as government ID programs), if there is no strong legal justification for collecting or receiving biometric data, then you may wish to reconsider the use of biometrics in your project.

Update Q2 in the biometric project planning template

For more information contact the Data Help Desk, Data Protection and Privacy Specialist, or Senior Advisor – Ethics in Evidence Generation

18. UNHCR's Guidance on the Protection of Personal Data of Persons of Concern to UNHCR provides a detailed explanation of consent and its application in the collection of personal information in humanitarian settings (72), as does the Handbook on Data Protection in Humanitarian Action (71)

© UNICEF/Abela Ralaivita



Q3 Is the biometric technology appropriate for the target age group(s)?

Current biometric technology has been developed primarily for use with adults, although there are a range of technologies under development for children. Focussing purely on the technology itself – there are a range of issues that affect whether a technology is suitable for use with children and adolescents (6). These include (and are summarised in Table 2):

- The permanence of trait being used (how much the trait changes over time). Many physical features change dramatically as children grow, making matching difficult, or requiring the template to be 'artificially aged' using further algorithms and estimation (see Question 4).[19]
- The ability to capture a clear image with enough detail for processing as a digital template. Among adults for example, iris recognition is considered one of the most accurate and inclusive biometric technologies, with lower rates of false accepts and rejects, and the ability to enrol more people than other traits (28). However, it is not considered suitable for use with newborns and infants, or young children, given the high level of cooperation required to obtain a high-quality image. Similarly, while fingerprints have been used extensively among adults, given the much smaller size of children's fingers, most standard sensors cannot adequately extract the features needed for template generation, even when the ridge structure is clear (18).
- User acceptability of the technology with the age group, or in the case of children, their parents or caregivers. For example, the use of DNA as a potential biometric trait has very low acceptability across all age groups, but especially for use with children who cannot provide informed consent for this level of data collection, and for whom the potential data risks could have lifelong consequences. Potential issues among older children – such as sensitivity for teenage girls if required to uncover for facial recognition etc. should also be considered.

Overall, very few biometric traits are suitable for use among newborns and infants, given the difficulties in capturing images of sufficient quality for use in automated systems (15). Similar challenges remain among young children, with the range of potential biometric traits for use expanding as age increases. Equally, as adults age – certain traits become harder to use accurately due to the natural ageing process, injuries and ailments such as arthritis (25, 73, 74).

19. Noting that the ability of algorithms to 'artificially age' templates is still very much in development, with varied levels of success. The reliance on algorithms to model and adjust for age also raises ethical concerns, especially regarding the potential of excluding children from services when biometric systems cannot match templates over time

TABLE 2. **CHARACTERISTICS OF BIOMETRIC TRAITS AND THEIR APPLICABILITY* WHEN WORKING WITH VERY YOUNG CHILDREN (LESS THAN FIVE YEARS)**

BIOMETRIC CHARACTERISTIC	FACIAL	FINGERPRINT	IRIS	PALMPRINT	FOOTPRINT	RETINA	HAND GEOMETRY	VEIN PATTERN	EARPRINT	DNA
UNIQUE/DISTINCT	L	H	H	–	H	H	M	M	–	H
PERMANENT	LM	M	H	M	M	MH	M	M	M	H
UNIVERSAL	H	M	H	–	M	H	M	M	–	H
MEASURABLE	H	M	M	–	M	L	H	M	–	L
PERFORMANCE	LM	MH	H	–	H	H	M	M	–	H
USER ACCEPTANCE	H	MH	L	MH	MH	L	M	M	M	L
CIRCUMVENTION**	L	H	H	–	M	H	M	H	–	H
LEVEL OF COOPERATION REQUIRED	M	M	H	H	H	H	M	H	M	H

Source: adapted from Jain et al, 2015 (18), Dinkar & Sambyal, 2012 (75), Kotzerke, 2014 (15); van Greunen, 2016 (12)
L = low; LM = low-to-medium; M = medium; MH = medium-to-high; H = high; – = no evidence
* Scores were allocated based on subjective reviews from four previous research articles; a single score (ie. 'M') represents all authors agree on the performance level, while a range ('LM') represents the different scores provided by different authors
**As this characteristic measures the difficulty in imitating or obscuring a biometric trait, a 'high' score represents high difficulty, while 'low' represents the trait is easy to imitate or obscure

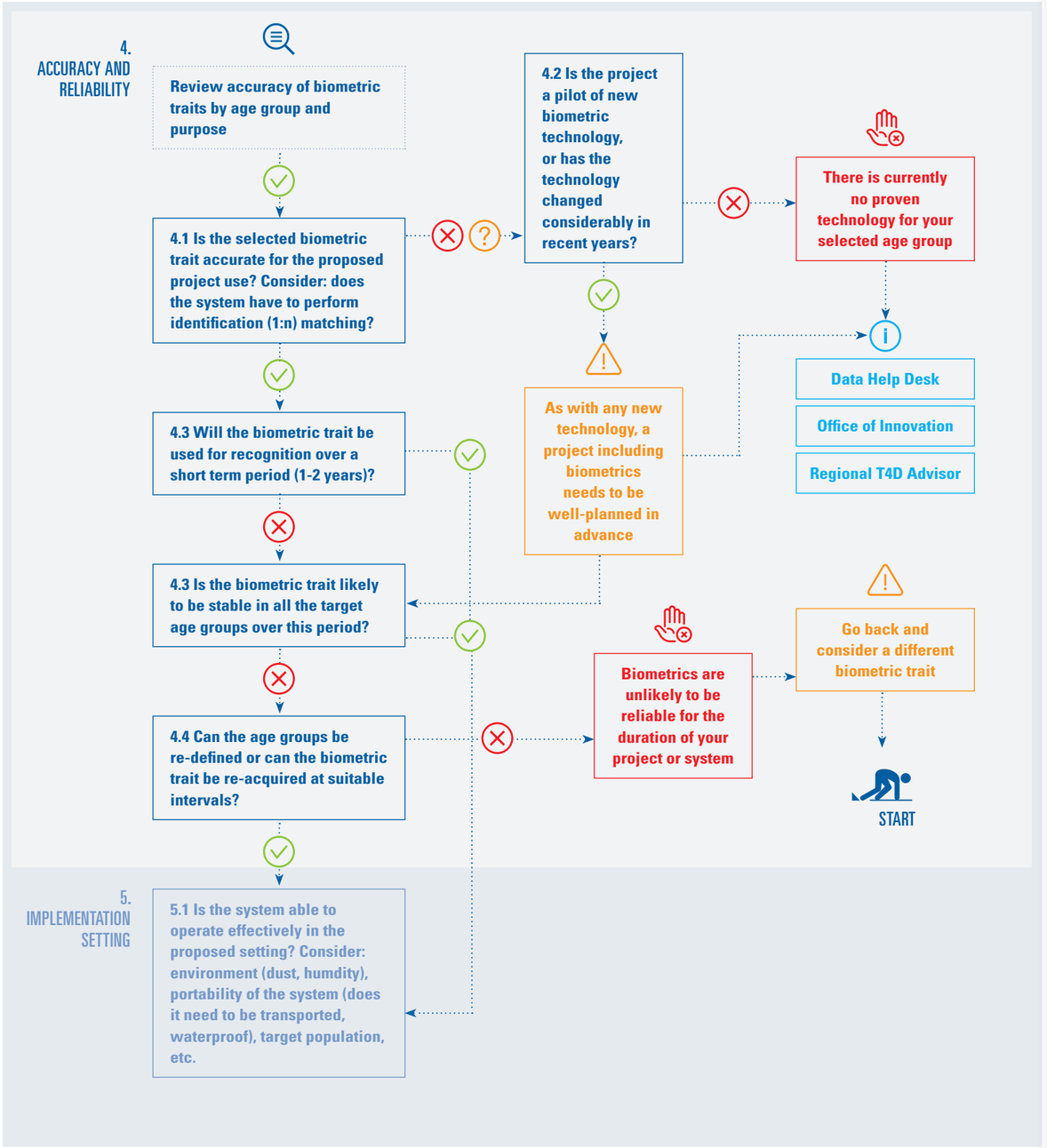
© UNICEF/jiroose@gmail.com

⚠ **Consider the age groups that your project intends to include, both at initial roll out and in any potential expansion of scope. If your project includes children less than five-years-old, proceed with CAUTION. Pending on the biometric trait selected, your project is likely to have high rates of 'failure to acquire' and/or 'failure to enrol' in the system; as well as problems with the accuracy of matching.**

Update Q3 in the biometric project planning template

For more information contact the Office of Innovation and/or Regional T4D Advisor

Ask potential vendors to supply the details of their performance metrics and supporting evidence



Q4 Is the biometric technology accurate and reliable for the proposed project use?

While the technology is rapidly improving, recognition rates among children (especially the youngest age groups) are consistently lower than for adults (6, 17). Vendors should be able to provide you with data on key performance metrics by age group for their system: if a system can only recognise a child 40, 50 or 60 per cent of the time (for example), is that enough? What other systems will need to be implemented when these rejections or system failures occur? Programs should query technology providers on how their thresholds are set, and what this means in terms of both recognition accuracy and errors. Vendors should be able to provide data on the performance of their system against accepted measures (as outlined below) and document the procedures that will be followed in case of system errors.

While many biometric technologies are well-established for adults, there is a lot less certainty on the accuracy and reliability of the technology in children, and the technological developments for use in children is much newer (30). The matching algorithms used in fingerprint recognition with children, for example, are based on adult fingerprint patterns and current research has highlighted their inability in using information contained in child prints, even those captured at high-quality (73). Growth itself is also a challenge to capturing and comparing physical features, especially in the first few years of life (5, 14), and this means that biometric technologies (designed to work with adults) are less accurate when recognizing children.

Accuracy

There are two major factors that affect the recognition accuracy of biometric systems: the **age of the person at enrolment**, and if the system needs to be able to **identify or authenticate individuals**, as some technology is better at this than others (6). The age of someone when they enrol in a biometric system has an impact on if they can provide a suitable image for enrolment, and on the quality of the image they can provide. For example, the skin of newborns often dries and peels soon after birth, and this distorts the image of print-based features (such as fingerprints, footprints and palmprints) (14). As children are also smaller than adults, their physical features also smaller, and this makes feature extraction more difficult.

There is also an important difference between authentication and identification in biometric recognition systems (10, 24). Authentication is the process where a user claims an identity and the system checks (accepts or rejects) if they are that user. It does this by comparing the most recent template provided with those already stored, in what is known as ‘one-to-one’ or ‘1:1’ matching (1, 2, 5). Individuals usually provide a unique identification number, username, or token, along with their biometric data to help the system find the relevant template and answer the question, ‘are you who you say you are?’ Authentication systems have mostly been used to prevent unauthorised people from accessing services they aren’t entitled to (5).

In identification, a user attempts to positively identify themselves without explicitly claiming an identity (2). They provide their biometric data and the system compares this with all the templates stored in the database to answer the question, ‘who are you?’ or more appropriately, ‘are you someone who is already in the system?’ (5). Identification systems are useful in preventing the same person from having multiple official identities; multiple credentials (such as a passport); or receiving multiple benefits (for example, state welfare or development aid) (5, 28). However, as the system must perform many more matches than when in authentication mode, the number of errors increases (1).

Recognition accuracy for authentication is primarily measured through the **true accept rate** (TAR),[20] which is the proportion of queries where the system is able to correctly match the biometric trait(s) for an individual to their identity information in the system (3). For identification, the primary measure is the **Rank-1 identification rate**.[21] This is the proportion of queries where an individual is correctly matched with a record in the data set and returned as the most likely candidate (5, 6). System performance for identification is dependent upon the size of the database, threshold level and number of possible identities returned (5, 24).

Accuracy over time: reliability

Recognition accuracy decreases as the time between enrolment and query increases (76, 77). This is due to physical or 'trait ageing': fingerprints deteriorate with age as their ridge structures lose definition; facial recognition is affected by a loss of elasticity, movement of the teeth and jaw, muscle wasting, and fat accumulation; and the ability of the iris to respond to light in the same way decreases with age (78). Certain groups of people may experience trait ageing at a different rate to others, such as manual labourers whose fingerprints may become more worn much more quickly (73).

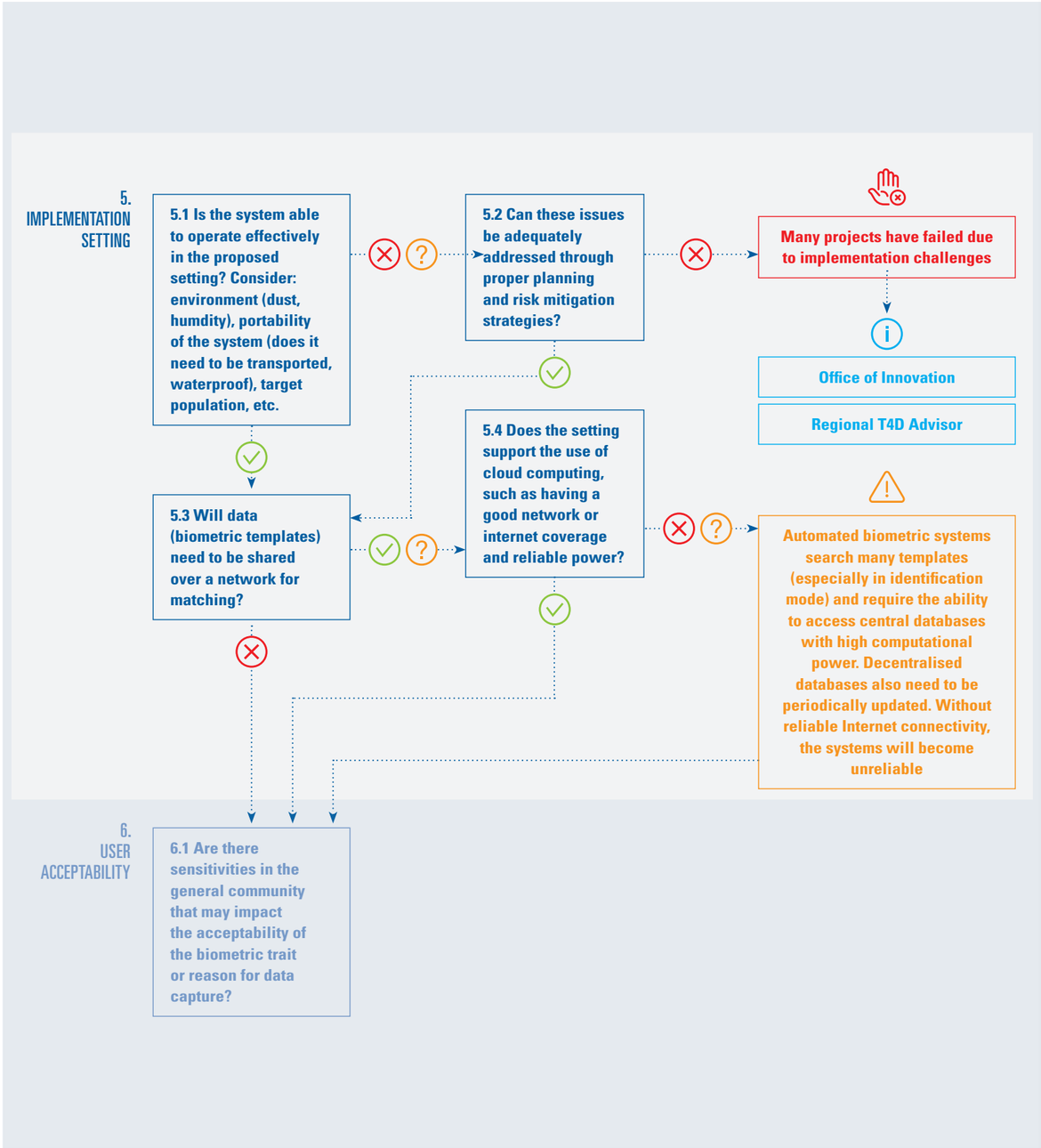
The reduction in accuracy can also be due to 'template ageing', which is a measure of the ability of biometric systems to recognize physical structures in the digital world over time (73) and account or adjust for the physical ageing process. The rapid changes in facial features that occur as young children are growing, for example, often means that their biometric templates become very dissimilar to their actual faces, very rapidly (78). While researchers have developed growth models to try and enhance the biometric templates of children, these models do not work very well (2, 14). There are also few large-scale, longitudinal studies on the performance of biometric systems among adults, and even less among children, making it difficult to fully understand how well they work over time.

If your project includes children less than five-years-old and needs to work in identification mode, pending the biometric trait selected, you may need to STOP at this point or re-assess the project. There are very few biometric technologies that are proven to work well among younger age groups, especially in identification mode

Update Q4 in the biometric project planning template

For more information contact the Data Help Desk, Office of Innovation and/or Regional T4D Advisor

20. The TAR is also referred to as the correct accept rate (CAR) and genuine accept rate (GAR)
21. Also referred to as the true positive identification rate (TPIR)



Q5 Is the technology suitable for the setting?

Few biometric systems have been built specifically for use in the developing world, or to deal with operating in rural, remote, and otherwise generally harsh environmental conditions (high temperatures, humidity and levels of dust) (40). Further, vendors often present evaluation results based on 'good' data, while in practice – due to various constraints and conditions – real operational data tends to be 'less good' (35). One large study, for example, tested six commercial sensors reporting high accuracy levels by collecting over 125,000 fingerprint images from low-resource populations, and every system tested failed to reach accuracy rates published in industry reports (40).

There is limited evidence on how well current technologies work in varied environments, or by user characteristics such as age, ethnicity, or occupation. One study looking at fingerprint recognition among young children (aged 0–4 years) included children from Michigan, USA, and Benin, West Africa (44). Authentication and identification accuracy were much lower for children in Benin: in some cases, as few as 30 per cent of children were successfully authenticated and 20 per cent identified (compared with 62 and 46 per cent of children from Michigan). This is likely due to the high-temperature and high-humidity setting of Benin, where much of the biometric enrolment was done in open-air settings, and the fact that the children in Benin were more likely to be younger than six months of age.

Another study reported on the overall poor performance of facial images collected during a cold winter day in India, due to children wearing hats that covered certain facial features, and the different level of sunlight (17). In the 2016 audit of UNHCR's biometric system;

> *The verification and enrolment of identities was generally fast (2 to 3 minutes per person in DRC and Thailand, and a bit longer in India due to* **low internet connectivity and difficulties in capturing data of children***)… The main problems reported by offices related to the fragility of iris scanners, and system failures due to* **fluctuations in the internet availability** *and* **repeated failed attempts** *to capture biometric data (pg. 8, emphasis added) (7).*

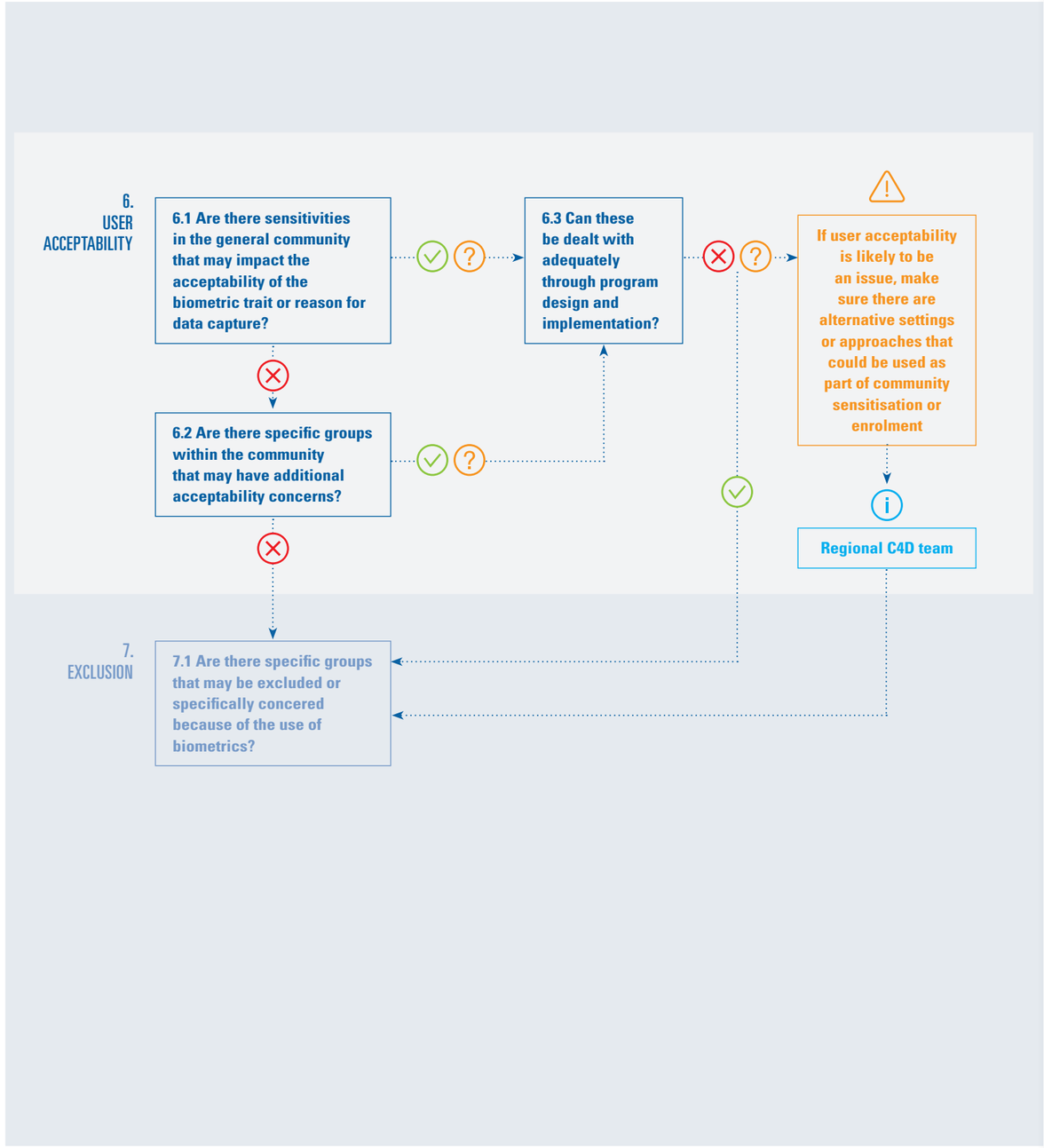
An important question to answer at the start of the planning process is if the system can operate effectively in the proposed setting. **Where will the data be collected** – how will this affect the quality of the images needed for enrolment and later for recognition? Does the technology need to be portable? What are the infrastructure needs, including access to power and Internet connectivity? What evidence of success is there for the system and by the vendor(s) under consideration, and is this evidence independent?

If your implementation setting has unreliable Internet connectivity, proceed with CAUTION. Automated biometric systems search many templates (especially in identification mode) and require the ability to access central databases with high computational power. Decentralised databases also need to be periodically updated. Without reliable Internet connectivity, the systems will become unreliable

If the selected system is not able to operate effectively in your project or program setting, it is recommended you STOP at this point and reconsider the use of automated biometric systems

Update Q5 in the biometric project planning template

For more information contact the Office of Innovation and/or Regional T4D Advisor



Q6 How acceptable are biometrics among the target community?

User acceptance of biometrics varies with case and context, and this means in some situations, otherwise effective biometric technologies can become inappropriate and potentially exclusionary. Programs and projects linked with rapid responses to food insecurity, for example, generally do not have the lead-time needed for community sensitisation or an assessment of Internet and power availability. This would mean trying to both provide necessary (often lifesaving) services, while enrolling people into a biometric system they are unfamiliar with. Also likely occurring in settings with no or very limited connectivity or electricity: increasing the chances of failed enrolments and recognition errors, and a poor user experience.

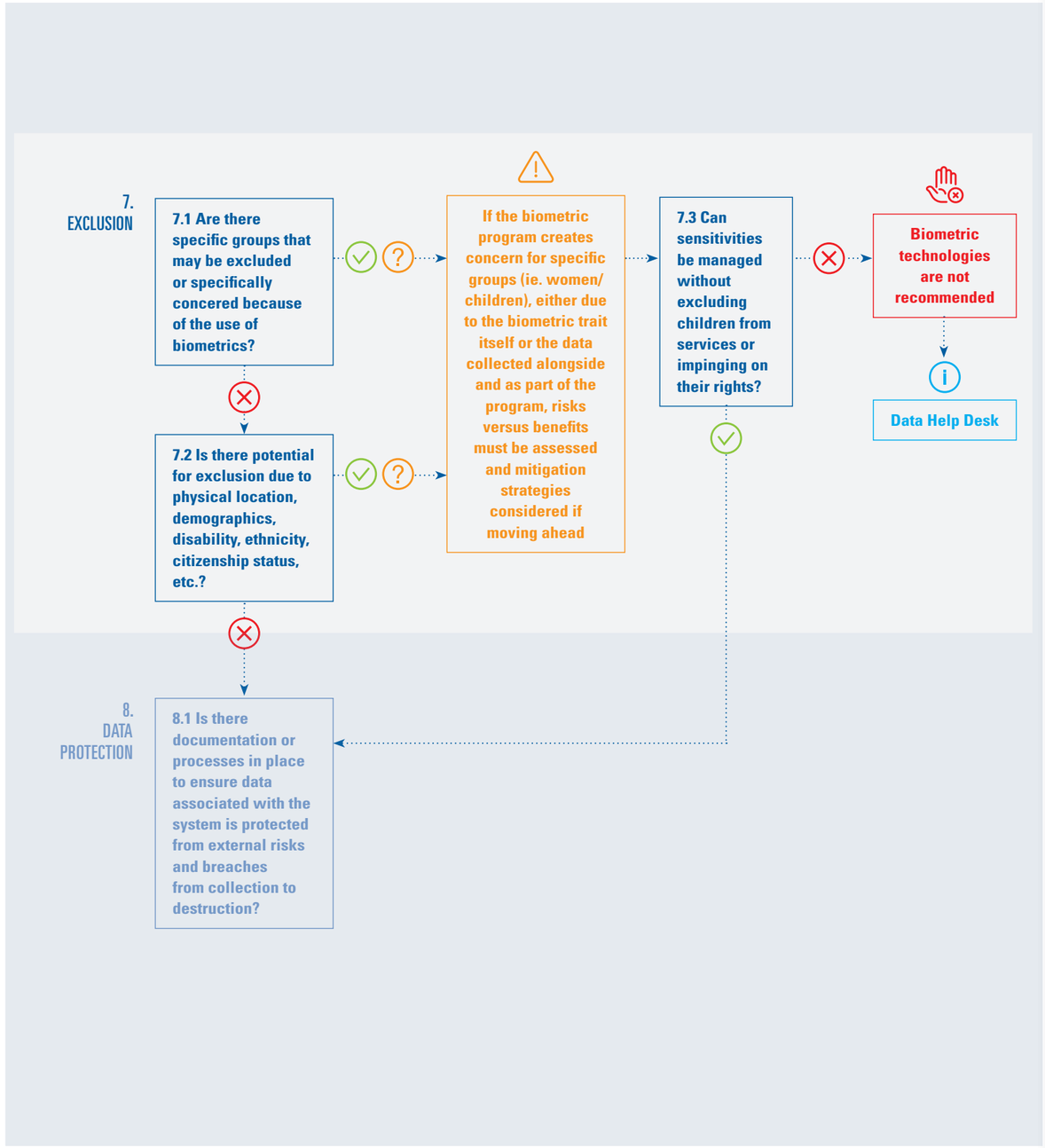
Such case-specific examples on acceptability are also located within the larger country (or region) context or setting. In Bangladesh, for example, while over 70 per cent of veiled Muslim women objected to having their iris scanned or photograph taken, the majority were willing to provide a fingerprint (34). A study in South Africa found high (over 90%) acceptability of the use of fingerprints in a healthcare setting among non-stigmatised populations, while in Rwanda, one study on the use of fingerprints in government-owned health facilities showed some concern among patients over improper use of their data by the government (79). In another study into the use of fingerprint recognition technology among female sex workers in Zambia (a vulnerable and stigmatised population) the authors found that less than half of the women were comfortable in providing their print in the field due to privacy and confidentiality concerns (79).

Consider: are there sensitives in the general community, or in specific groups within the community, that may impact on the acceptability of the biometric trait selected, or use of biometric recognition more generally? Can these be dealt with adequately through program design and implementation? Are there alternative settings or approaches that could be used regarding community sensitisation or enrolment in the system? Careful consideration should be given when these systems are targeting especially vulnerable communities or larger data sets that capture characteristics that could be used to identify these individuals or groups.

If there are sensitivities in the community around the use of specific biometric traits or biometric systems more broadly, or issues that may prevent you from adequately engaging with the community, it is recommended you proceed with CAUTION

Update Q6 in the biometric project planning template

For more information contact the C4D teams in your region



Q7 Could the introduction of biometrics potentially exclude children or families from services or protection?

One of the biggest concerns around the use of biometric technologies is the risk of exclusion. The risk comes from the potential these systems have in excluding certain groups from services and benefits they are otherwise entitled to (38). The exclusion can be systematic, due to poor planning or targeted policies of exclusion; or it can be incidental, when a system fails to enrol a person or comes back with a false accept or reject. Both require the establishment of policies and procedures to remedy and mitigate potential exclusion (Box 11). Having effective and responsive grievance processes, and fast and effective support to deal with technical failures are critical in ensuring that the technology does not increase the risk of exclusion for any user, or group of users.

The risk of exclusion is of high concern for children, as there is limited evidence that biometric technology has developed enough to capture and match child biometrics (18). Recent approaches to establishing national identity systems based on biometrics for adults in the absence of a strong link to civil registration potentially result in weakening of the registration system and subsequent exclusion of children; and increases the potential of 'open' or fraudulent identities in the absence of strong links to death registration (1). Apart from age, other potentially exclusionary characteristics include gender (29), ethnicity (37), disability (38), and occupation (5).

Ask yourself: are there specific groups that may be excluded or specifically concerned around the use of biometrics? This includes people whose biometrics can't be recorded and are excluded from services; system errors that may result in temporary or permanent exclusion; and self-exclusion (opting out in order to avoid issues/embarrassment). In addition, if biometrics are used to limit the amount of other personal or identifiable data that is shared during a transaction or data exchange, we need to consider if reduced data disaggregation as a result of this more limited data set could potentially conceal the extent of any exclusion.

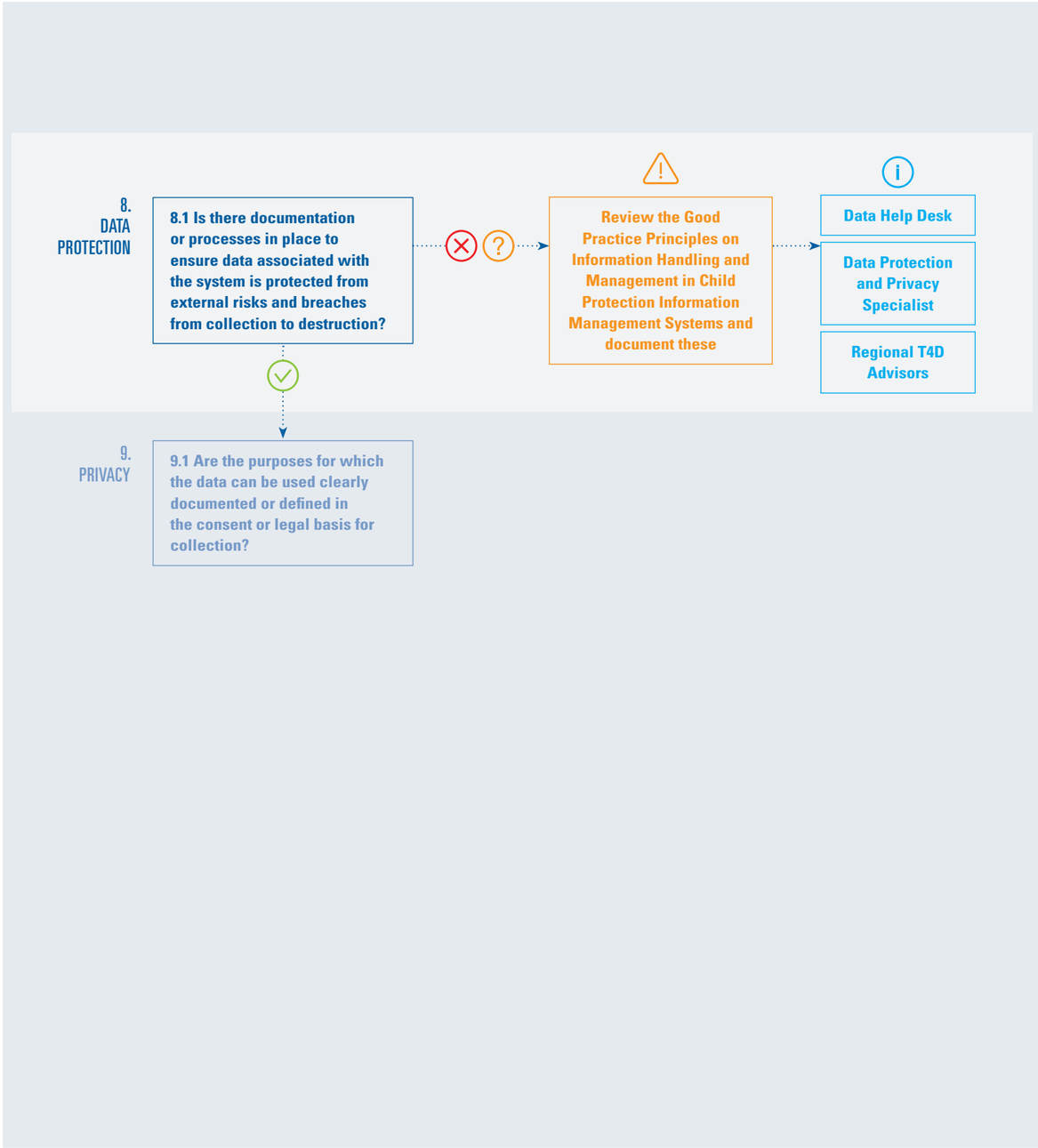
BOX 11. AADHAAR'S APPROACH TO INCLUSION

By law, the Aadhaar system is required to enrol everyone: if fingerprints cannot be collected, policy dictates that iris scans be collected; if iris scans cannot be collected, a photograph is taken instead and an Aadhaar number will be issued based on biographical information (80). The system operator must also make notes in the system on if the inability to provide a specific trait is due to permanent disability (such as amputated fingers) or due to temporary issues (sensor conditions, etc.) and if re-enrolment with biometric data can happen later.

If the potential for exclusion cannot be managed, it is recommended you STOP at this point

Update Q7 in the biometric project planning template

For more information contact the Data Help Desk, and/or Senior Advisor – Ethics in Evidence Generation



Q8 Can the data be appropriately protected at all stages from collection (or receipt) through to destruction?

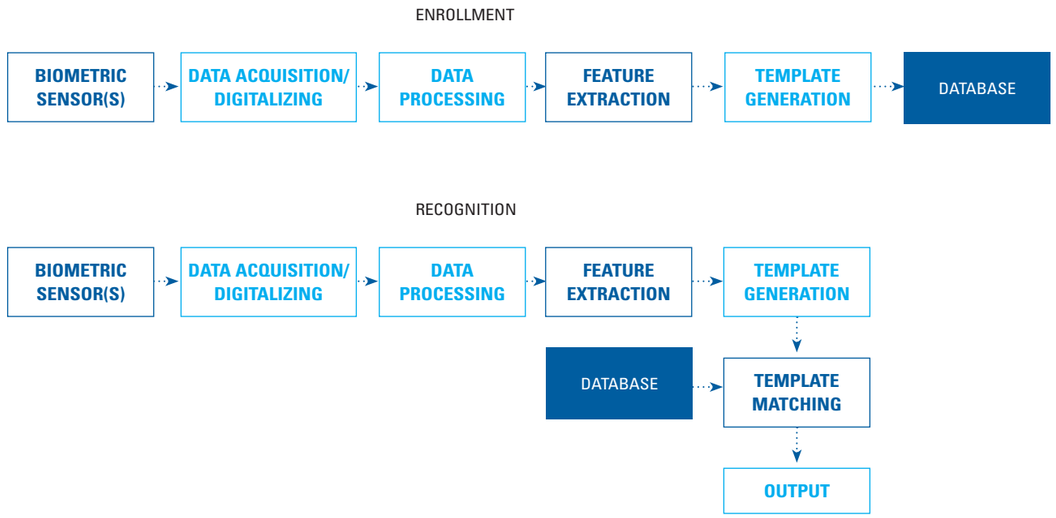
As with any technology, there are risks and vulnerabilities associated with biometric technologies at each stage as data moves through the system (Figure 4) (81). During enrolment, for example, biometric data is often recorded along with biometric data (name, date of birth, etc.), increasing the risk of being able to identify specific individuals if the data is ever abused, lost or stolen. Once processed into a template, it is possible to 'reverse engineer' biometric data back into original images, for example from an 'Iriscode' back to an image of an iris (27). While these 'recreated' images may not look like the original, they still contain enough information in them to be positively identified with the original user. Finally, the storing of large amounts of personal data in large databases also creates additional privacy risks, especially if the data is ever misused, such as if a host country was to request or demand humanitarian data to repurpose for law enforcement (34, 82).

Systems are particularly vulnerable at the sensor level (used to measure and record raw data) (5), and 'attacks' can come in many forms, from having false biometric data presented by an imposter; digital recording devices attached to record and reconstruct input data; hacking of the storage system; to physical attacking or tampering with the hardware of the sensor itself (24).

These fraudulent practices, known as 'spoofing' are considered more difficult than password theft (83), but can still occur. Four main areas of attack have been described (84), specific to biometrics and beyond the normal risks of data protection and broader social and ethical concerns:

1. **Tampering**. This is when a hacker provides false biometric data to a sensor, for example by using a silicon finger, or a photo of an eye for iris recognition.
2. **Retransmission of information**. This can occur at many points through the process, for example between the sensor and pattern extractor, template extractor and matcher, database and verification system, and point of registration and database. The aim of such attacks is to replace genuine user information with that of an imposter.
3. **Engineering analysis**. In these types of attacks, a virus may be aimed at the extractor to generate predetermined values, or the matcher may be attacked and altered to only provide exceptionally high or low values.
4. **Database manipulation**. The database may be hacked in order to destroy, damage or steal user's information.

FIGURE 4. DIAGRAM FOR A TYPICAL BIOMETRIC SYSTEM (SIMPLIFIED) SHOWING ENROLMENT AND RECOGNITION



Source: adapted from Du, 2013 (24)

Before implementation, be sure to check if there is documentation or processes in place to ensure data associated with the system is protected from external risks and breaches through all steps in the system, and from collection to destruction. Documentation should consider the following (Box 12):

- Has the decision on whether to store the data in a centralised or decentralised database been made?[22]
- What are the retention and destruction practices?
- How might individuals be affected if their data is compromised?
  - What is the likelihood of the risks? What is the range of possible adverse outcomes from least to most severe?
- Have staff been trained in requirements for protecting personal information and are they aware of policies regarding breaches of security or confidentiality? Are there plans for updated training as a result of the project under review?
- Are there authorisation controls defining which staff may add, change or delete information from records?
  - Are there clear guidelines on the physical location for the hardware and/or software through which data can be accessed? Is multi-factor authentication required for access to the system?
  - Is the system designed so that access and changes to data can be audited by date and user identification?
  - Does the system "footprint" inspection of records and provide an audit trail?
  - Are user accounts, access rights and security authorisations controlled and recorded by an accountable systems or records management process?

BOX 12. UNITED NATIONS COMPENDIUM OF RECOMMENDED PRACTICES FOR THE RESPONSIBLE USE AND SHARING OF BIOMETRICS IN COUNTER-TERRORISM

The UN Compendium offers several examples of good practice in relation to data protection, including:

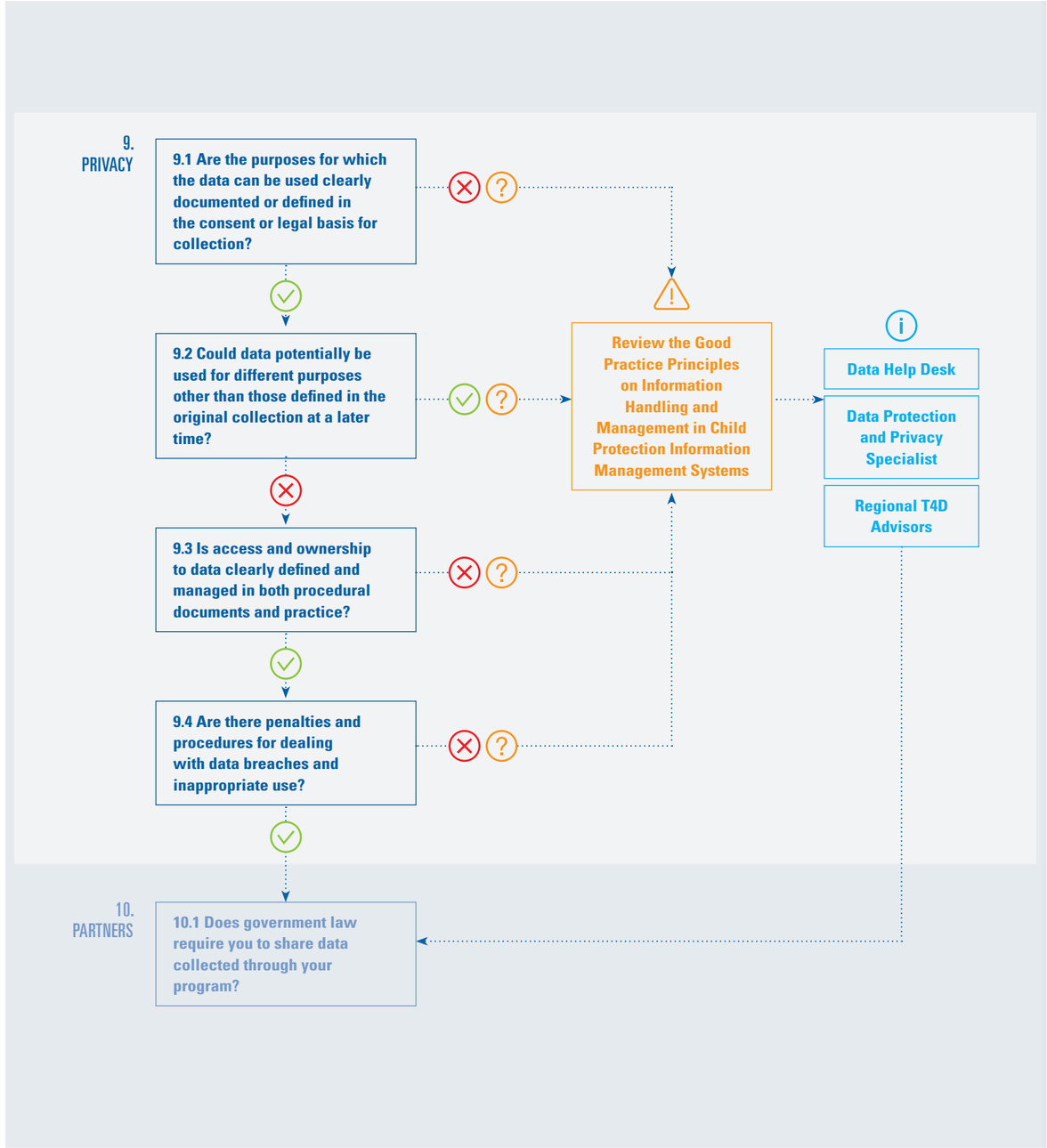
- Store biometric data separately from its related biographic data
- Only permitting senior-level staff to access biometric and/or biographic data, and ensuring there is a formal record of that access, and why access was sought
- Requiring biometric data of staff accessing the system
- Having more than one person within the organisation responsible for the validation or revocation of records
- Nominating a data controller who is responsible for managing all data processing activities

- Are there adequate ongoing resources budgeted for security upgrades with performance indicators in systems maintenance plans?
- Will personal information be transferred outside of the country? If so, outline aspects of the transfer including details of the receiving country. Explain steps to be taken to protect the information and the interests of the people concerned.

Update Q8 in the biometric project planning template

For more information contact the Data Help Desk, Data Protection and Privacy Specialist, and/or Regional T4D Advisors

22. There is no 'one-size-fits-all' solution to this issue. Centralised databases (storing all the templates in one place) can increase security by having physical isolation and strict access control. However, the compromise of a central database would have far greater implications than the compromise of one, local, decentralised database (5)



Q9 Can data privacy concerns be appropriately managed?

Privacy is a right[23] and a wider concept than data protection. Privacy advocates have raised concern over new applications of biometrics, over and above pre-existing risks that relate to identity theft and the misuse of personal information (53), given the richness of information that biometrics provide, which have much greater consequences when misused, abused, lost or stolen (34). Broad areas of concern relating to the use of biometric technologies and privacy include who can access the data and for what purposes, and the amount of data associated with the biometric template (ie. name, date of birth, other potentially sensitive information regarding ethnicity, religion, etc.).

Consider if the purposes for which the data can be used are clearly documented or defined (Box 13). While the idea of collecting as much data as possible and keeping it for as long as possible, in order to do as much good as possible, may seem acceptable – it is not (80). Obtaining and retaining personal information is always an interference with privacy rights, and the benefits must be weighed against the risks (64). The European Union's Data Protection Regime refers to this as the **principle of proportionality**: only collecting enough data that is proportional to what the project or organisation wants to achieve (85).

How long will data be retained for? It is important not to keep data past its operational usefulness because it might become useful in an unspecified way at an unspecified time in the future. Maintaining a 'lean' dataset is an important line of defence against mission creep, with creep more likely to occur if more data is collected than needed and kept for longer than needed (64). This approach also reduces the risk of loss or theft of the data.

In thinking about who can access the data, consider the following:

- Which staff, classes of personnel, agents or contractors will have access to the information? For what purposes? How will the access or disclosure be controlled?
- Will the data contain personally identifiable information?
- Are access rights only provided to users who require access for the stated purposes of collection or consistent purposes? Is user access to personal information limited to that required to discharge the assigned functions?
- Are the security measures commensurate with the sensitivity of the information recorded?
- Are there contingency plans and mechanisms in place to identify security breaches or disclosures of personal information in error? Are there mechanisms in place to notify security breaches to relevant parties to enable them to mitigate collateral risks?

23. Article 12 of the Universal Declaration of Human Rights: 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.'

BOX 13. PRIVACY IMPACT ASSESSMENTS AND NOTICES

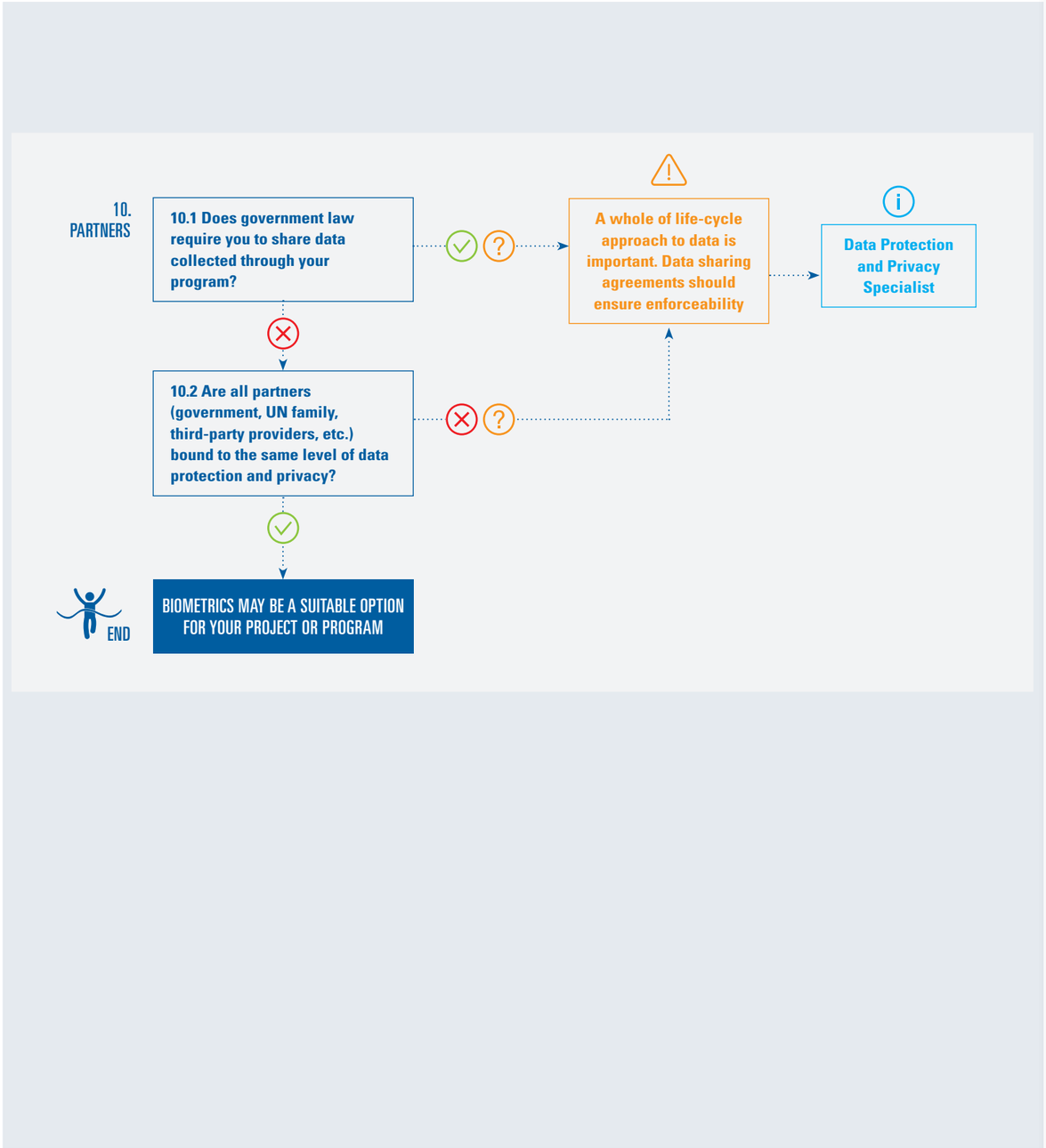
A data protection and privacy impact assessment (DPIA) aims to; 'identify, evaluate and address the risks to Personal Data arising from a project, policy, programme or other initiative. A DPIA should ultimately lead to measures that contribute to the avoidance, minimization, transfer or sharing of data protection risks. A DPIA should follow a project or initiative that requires Processing of individuals' data throughout its life cycle. The project should revisit the DPIA as it undergoes changes or as new risks arise and become apparent' (71). These assessments also aim to identify the roles and responsibilities of all stakeholders involved, guarantee accountability, and adopt a beneficiaries' rights-oriented approach.

Creating **privacy notices** can also be useful (86). Privacy notices summarise all the ways that data may be used or shared. They are done for the benefit of individuals by providing them with the necessary information to make informed choices. Privacy notices also ensure a more disciplined approach within an organisation when thinking about privacy, as organisations must think about issues around data uses and sharing when developing one. Once data has been collected, any subsequent use or sharing that was not in the original privacy notice must be justified on several bases, including consent and that the new uses are legitimate and enough to outweigh any potential risks.

© UNICEF/Santiago Arcos

Update Q9 in the biometric project planning template

For more information contact the Data Help Desk, Data Protection and Privacy Specialist, and/or Regional T4D Advisors



Q10 Are potential partners and implementing agencies equally committed to data protection and privacy measures?

UNICEF is often required to process personal data of vulnerable persons, notably children, including to share (and receive) such personal data with implementing partners and/or third parties. While implementing partners are often defined in concrete terms,[24] the notion of a 'third party' reflects the large variety of actors UNICEF collaborates with, including governments, data processing service providers, universities and/or individual researchers, and the private sector. While this data sharing is important, it also creates additional data security and privacy risks. Special consideration also needs to be given to third-parties, particularly private sector entities, that may work with implementing partners and have access to data through the provision of biometric linked services (such as the delivery of cash payments); the actual provision of the technology or maintenance of a biometric database; or through technical support to partners. Project managers should clearly understand all the potential access points to the data so that appropriate decisions can be made and potential risks mitigated.

UNHCR's Guidance on the Protection of Personal Data (72) outlines a series of practical questions in assessing the risks associated with data sharing, including:

- Does the implementing partner and/or third party respect the basic principles of personal data processing (as outlined by the OECD, for example, proportionality, confidentiality, data security, etc.)?
- Is the level of data protection afforded by the partner and/or third party at the same level as UNICEF?
- What is the legitimate and specific need of the data transfer?
- Could the transfer of data negatively impact the safety of either UNICEF personnel, or the individuals from whom the data was collected from?

Overall, ask yourself: does government law require you to share data collected through your program or project? Are all partners bound to the same level of data protection and privacy? Having clear data sharing agreements is one way to ensure accountability between partners, by setting out the terms and conditions for the use of the data, including an obligation to maintain the confidentiality of the dataset and prevent unauthorized access.

To ensure adequate protection during data sharing, The Handbook on Data Protection in Humanitarian Action (71), also suggests the following steps should be followed:

- any data protection rules or privacy requirements applicable to the data sharing (including any data protection or privacy requirements of local law, if applicable) have been satisfied prior to the transfer; and
- a legal basis must be provided for the transfer; and
- a DPIA (see Box 13) should be carried out to determine that the transfer does not present unacceptable risks for the individual (eg. discrimination or repression); and
- the organization that initiates the transfer must be able to demonstrate that adequate measures have been undertaken to ensure compliance with the data protection principles set forth in this Handbook by the recipient entity in order to maintain the level of protection of Personal Data with regard to International Data Sharing (accountability); and
- the individual should be informed about the recipient(s) of the transfer. The transfer should not be incompatible with the reasonable expectations of the individuals whose data are transferred.

Update Q10 in the biometric project planning template

For more information contact the Data Protection and Privacy Specialist

24. And may include, for example, UNICEF offices operating in different countries, and other NGOs, International Organizations and United Nations agencies

SECTION IV

Moving towards implementation

Once it has been decided to move forward with biometric technology, teams will need to ensure that the ethical issues and protections worked through in the assessment phase are carried through into implementation. There are also a range of additional issues that should be considered in this planning phase that are worth noting here.[25]

Overall, it is important to remember that biometrics are a tool for identity management systems, situated within a broader context of increased demands for reliable identification and rapid technological growth (87, 88). This has led to increased pressure to use biometrics and other technological innovations in a broad range of applications. This pressure exists despite the lack of large-scale studies on effectiveness; a relative lack of evidence that the technologies actually solve many of the problems they aim to address; a high degree of speculation; and numerous social, ethical and data risks and concerns (4, 34). As commented:

> *'…the current landscape of biometric projects is littered with pilots that have been unable to scale through issues including low accuracy performance, high costs and low interoperability between vendors' (pg. 5) (12).*

System cost and sustainability

Total cost of ownership includes up-front system costs related to the purchase and installation of equipment, training, documentation and potentially costs associated with system changes or upgrades required to integrate the biometric technology into existing systems. Ongoing costs include software and system licencing, hosting, administration and user access control, security, maintenance and 'bug fixes', as well as ongoing training support and management to ensure that the system is sustainable over the long term as individuals engaged in the delivery, maintenance or oversight of the system change. Ongoing costs should also factor in items such as ongoing data storage and security – including the need to continually upgrade systems to address evolving security risks.

Sustainability of the system is essential given the highly personal nature of the data being collected and stored. This should closely consider inter-operability with other systems already in place or planned in the proposed setting and include a plan for decommissioning or retiring data from the system and associated costs.

25. Additional resources and guidance will be developed and made available through the Data for Children website

The system, technology, and user interaction

Biometric technology is changing rapidly, and as such –key features, performance measures and portability of equipment are continually evolving. Teams will need to work closely with vendors to understand proposed systems capabilities and the evidence or testing that exists to support these claims, and to evaluate how considerations outlined relate to the specific technology proposed. It will also be necessary to continually review security requirements and risks and ensure that these are factored into forward planning.

Some of the key technological considerations at implementation include (1, 33):

- **Overall system design and the broader IT ecosystem**. Overall, the system should be integrated as part of end-to-end solutions and not as a stand-alone. The information technology 'ecosystem' must be assessed, including aspects such as access to a stable power supply and Internet connectivity and local IT support.
- **Vendor selection**. A large part of all biometric recognition systems remain within 'vendor-specific black boxes' (35) (Box 14). This makes it difficult to understand the full scope of intermediate steps within the broader processes, and particularly difficult to understand the limitations of each step when comparing with other vendors and systems.
- **Ease of use**. Noting there is usually a practical trade-off between complexity and security, and that training will be required for staff on how to use the system.
- **User acceptance**. The perceived or actual obtrusiveness and intrusiveness of the system (especially the sensor) is subjective and varied pending on context. In high security settings, for example, users may accept more cumbersome processes as they feel safer and more robust. The enrolment process should be non-invasive and socially acceptable, with sensors robust and able to cope with practical capture challenges, and the biometric trait itself easy to capture with consent (14). Engagement and communication with the target audience and broader community are important aspects in ensuring users are adequately informed and aware of the project.

BOX 14. THE DANGERS OF VENDOR 'LOCK-IN'

'Commercial extraction and matching algorithms are closed-source and proprietary. This makes them hard to upgrade or modify to meet project needs, limits the scope for collaboration, and makes the implementing organisation completely dependent on the vendor. **If the supplier stops supporting a system, or goes out of business, the project fails**' (pg. 8, emphasis added) (40).

And as reflected by the UN Secretary-General in 2009 on the extensive use of biometric technologies in national voting systems:

'Some of the poorest countries in the world have chosen some of the most expensive electoral processes and technology… I am concerned about techniques and systems that might cause a State, in the conduct of its own elections, to be financially dependent on donors, or **technologically dependent on specific vendors** for extended periods' (pg. 8), emphasis added (52).

Information technology 'ecosystem'

What is often lacking in many operational settings is the 'ecosystem for recognition', such as an adequate number of sensors at the point of service, or appropriate databases for template storage (Box 15). Emphasis is mostly on checking the validity of the credential, while other factors such as measures of total system performance, such as time for enrolment (12 seconds versus three minutes), additional computational requirements based on number of enrolled users, and performance across networks, are lacking (5, 10). A broader understanding of service-level requirements with any biometric system is needed, including throughput (transactions per hour), response time, and accuracy (4) for example. As noted earlier, independent verification of vendors' claims is ideal, as research shows that many self-assessed performance and accuracy data have not matched vendor marketing and claims.

One of the most important technical decisions is if the biometric data (including templates and any raw images) will be saved in a central or decentralised database. This decision may be impacted by how the biometric is intended to be used. Centralised databases are generally better for security, as they can be physically isolated from where enrolment and identification/verification take place, and it is easier to implement measures such as access control and regular maintenance of the hardware and software. However, as centralised databases contain all of the data in one place, if they are ever compromised, the outcomes are far worse than for a decentralised database (which may only have, for example, data on individuals who have been in contact with a specific health centre or school, rather than the whole enrolment database) (5).

BOX 15. PLANNING FOR THE TECHNOLOGY ECOSYSTEM

During Kenya's 2012 elections many of the supplied biometric kits failed to recognise voter's thumbprints, meaning their details had to be manually entered into the system. The classrooms used as polling stations also did not have power sockets, many of the voting officers forgot their identification numbers and couldn't access the system, and the system also simply failed to function on several occasions (89). Planning for challenges when using advanced technologies in developing countries is a critical part of any project and having viable back-up plans in the case of technological failure is key.

The frequent lack of connectivity in Angola, for example, has made off-line authentication necessary, leading to the deployment of mobile data capture and card issuance units for their biometric system (8). Data from the mobile units are sent to the central database via a secure satellite transmission or uploaded in batches. Similarly in Benin, mobile voter enrolment units were developed that were small enough to fit into a suitcase and came equipped with a laptop, camera, fingerprint scanner, printer, and signature pad, along with a separate generator (8).

Community engagement and communication

As with any new technology, it is important that communities are engaged in the process and are appropriately communicated with before, during, and after implementation of biometric technologies. What this communication looks like will depend on context and target audience but should include key aspects such as: what data is being collected and for what purpose; how the use of biometrics is of benefit to individuals and the community; and where people can go for more information.

© UNICEF/UN0261309/Sokol

Governance and coordination

This includes aspects around system design (including privacy provisions), support and workarounds in the case of system failure, and procedures for complaints, audit and review. Issues that need to be worked through prior to implementation include data ownership and access, accountability and follow-up (including provisions for audit, if applicable),[26] and sustainability (and long-term oversight of data once the project ends if applicable).

A special note on piloting new technologies

This resource is specifically intended to support teams to work through decisions related to whether to include biometric technology in our general programming, or to support partner agencies and governments in doing so. While some of these deployments are very likely to require a specific testing or piloting stage to evaluate whether the approach makes sense for that specific context or problem, this guidance is not intended to fully address the use of new, untested, or unproven technologies. In this context the project should be considered research, and should be both assessed and discussed with partners, governments and participants as such. Research proposals should also go through the appropriate ethics review mechanisms.

Critical considerations in this context will include the importance of well-informed, genuine consent procedures and appropriate options for "opting-out"; and clarity around both the role of UNICEF in the research and the limitations or "unknowns" of the technology being tested. It is recommended that research proposals are discussed with the Senior Advisor – Ethics in Evidence Generation (see contact list).

26. Reports from The Office of Internal Oversight Services (OIOS), Internal Audit Division, on UNHCHR's biometric identity management system are a valuable resource and good example of the importance of formalised audit processes

SECTION V

Next steps, research priorities and resources

Research priorities and next steps

UNICEFs engagement with biometric technology is very new, and there are significant gaps in the evidence that exists to inform our decisions. At the same time – the range of use cases that are relevant to our work is very varied (much broader in fact than many of our partner UN agencies), each posing their own set of additional considerations and questions. Complicating these challenges is the very fast pace of development of biometric technology has meant that much of the conversation (and indeed the expertise) has been led by industry, and the border management and public safety sectors; with less engagement from humanitarian and development partners beyond their own internal systems.

Overall, there is very little publicly available evidence on the recognition accuracy of biometric systems, or on the practical and ethical considerations when using such systems with children. Evidence is heavily focused on newborns and infants (<12 months), with very little data available on young children (1–4 years), older children (5–12 years), or adolescents (13–17 years). The data that is available shows that recognition accuracy is affected by choice of matching algorithm, and the accuracy of a system changes over time, especially for children due to their rapid growth. There has also been limited attention to the impact of biometrics, that is, whether use of the technology has changed outcomes, especially for children; with very few evaluation reports available on the use cases reviewed. While it is acknowledged that industry and various government and donor organizations are likely to have more evidence than what is published; the fact remains that very little of the research is becoming publicly available.

Given the rapid growth in biometrics, there is also a lack of global standards on the best use of such technologies, especially when applied to vulnerable groups such as children. However, work is happening through several UN collaborations, and there is a range of existing standards that can inform the use of new technologies and data principles more generally, even in the absence of specific guidance on biometrics. Priorities for UNICEF for future development include:

- Understanding the potential use cases of biometric technologies and impact of these.
- Building out implementation guidance as we learn from other agencies and across our organization.
- Generating consistent messaging on what we mean by appropriate use of biometrics – especially with children.
- Building capacity across the organization to engage with vendors, governments and partners on these emerging issues.
- Understanding the evolving technology of biometrics for children,[27] and where appropriate – working with partners to evaluate new options that meet specific program needs.
- Ensuring that biometric-based national identification systems are part of a whole of life-cycle approach to legal identity (ensuring a link with civil registration and birth registration).
- Addressing research questions such as the stability of infant biometrics across an individuals' lifetime.

27. Excluding DNA as noted in Section I

CONTACTS: WHERE TO GO FOR HELP

Additional resources will be added as they are developed, and can be found on the Data for Children site: https://unicef.sharepoint.com/teams/DRP/DataforChildren/SitePages/Data%20for%20Children.aspx

People to talk to:

Data for Children Helpdesk	dataforchildren@unicef.org
Administrative Data Specialist – Karen Carter	kcarter@unicef.org
Statistics Specialist (Household Surveys) & focal point for Ethics, Data and Analytics- Shane M Khan,	smkhan@unicef.org
Data Protection and Privacy Specialist – Sophie Clavet	sclavet@unicef.org
Child Protection Specialist- Legal identity and birth registration – Kristen Wenz	kwenz@unicef.org
Senior Advisor for Innovation – Tanya Accone	taccone@unicef.org
Senior Advisor – Ethics in Evidence Generation – Gabrielle Berman	gberman@unicef.org

You may also find it useful to connect with your regional T4D and C4D focal points in working through this resource.

REFERENCE LIST

1. Gelb A, Clark J. Identification for development: The biometrics revolution. Working Paper 315. Washington, DC: Centre for Global Development; 2013.
2. Jain AK, Nandakumar K, Ross AA. 50 years of biometric research: Accomplishments, challenges, and opportunities. Pattern Recognition Letters. 2016;79:80-105.
3. UNOCT, CTED. United Nations Compendium of recommended practices for the responsible use and sharing of biometrics in counter-terrorism. New York, USA: United Nations Office of Counter Terrorism and Counter-Terrorism Committee Executive Directorate; 2018.
4. World Bank. Technology Landscape for Digital Identification. Washington, DC: The World Bank Group; 2018.
5. Jain AK, Ross AA, Nandakumar K. Introduction to biometrics. New York: Springer; 2011.
6. Jain AK, Arora SS, Cao K, Best-Rowden L, Bhatnagar A. Fingerprint Recognition of Young Children. IEEE Transactions on Information Forensics and Security. 2017(7):1501.
7. OIOS. Audit of the Biometric Identity Management System at the Office of the United Nations High Commissioner for Refugees. Office of Internal Oversight Services, Internal Audit Division; 2016. Contract No.: Report 2016/181.
8. World Bank. The state of identification systems in Africa: Country briefs. Washington, DC: World Bank Group; 2017.
9. Berman G, Albright K. Children and the Data Cycle: Rights and Ethics in a Big Data World. Florence: UNICEF Office of Research; 2017. Contract No.: WP-2017-05.
10. Ashbourn J. Biometrics. Advanced identity verification: The complete guide. New York: Springer; 2000.
11. Pugliese J. Biometrics: Bodies, technologies, biopolitics. New York: Routledge; 2010.
12. van Greunen D. Ethics, children, and biometric technology. IEEE Technology and Society Magazine. 2016;35(3):67.
13. Mordini E, Petrini C. Ethical and social implications of biometric identification technology. Annali Dell'istituto Superiore Di Sanita. 2007;43(1):5-11.
14. Kotzerke J. BioTwist: Overcoming severe distortions in ridge-based biometrics for successful identification. Netherlands: University of Twente; 2016.
15. Kotzerke J, Arakala A, Davis S, Horadam K, McVernon J. Ballprints as an infant biometric: A first approach. IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications (BIOMS); Rome, Italy; 2014.
16. Ricanek K, Bhardwaj S, Sodomsky M. A review of face recognition against longitudinal child faces. 14th International Conference of the Biometrics Special Interest Group (BIOSIG); Darmstadt, Germany; 2015.
17. Best-Rowden L, Hoole Y, Jain AK. Automatic Face Recognition of Newborns, Infants, and Toddlers: A Longitudinal Evaluation. International Conference of the Biometrics Special Interest Group (BIOSIG); Darmstadt, Germany; 2016.
18. Jain AK, Arora SS, Best-Rowden L, Cao K, Sudhish PS, Bhatnagar A. Biometrics for Child Vaccination and Welfare: Persistence of Fingerprint Recognition for Infants and Toddlers. MSU Technical Report MSU-CSE 15-7. Michigan: Michigan State University; 2015.
19. de Paula Lemes R, Pamplona Segundo M, Bellon ORP, Silva L. Dynamic Pore Filtering for Keypoint Detection Applied to Newborn Authentication. 22nd International Conference on Pattern Recognition, Pattern Recognition (ICPR); 24-28 Aug.; Stockholm, Sweden; 2014.
20. Ramachandra R, Raja KB, Venkatesh S, Hegde S, Dandappanavar SD, Busch C. Verifying the Newborns without Infection Risks Using Contactless Palmprints. International Conference on Biometrics (ICB); 20-23 Feb.; Gold Cost, Australia; 2018.
21. Wong J, Koswin K, Sheikh A, Boychuk N, Assefa E, MacLeod M, et al. Case study: UNHCR Jordan's biometric cash assistance program for Syrian refugees. Canada: The Reach Project, University of Toronto; 2017.
22. UNHCR. Biometric Identity Management System. In: UNHCR, editor.
23. World Bank. ID4D Country Diagnostic: Peru. Washington, DC: World Bank; 2016.
24. Du EY. Biometrics: From fiction to practice. Singapore: Pan Stanford; 2013.
25. Grother P, Ngan M, Hanaoka K. Ongoing Face Recognition Vendor Test (FRVT). Part 2: Identification. Maryland, USA: National Institute of Standards and Technology; 2018. Report No.: NISTIR 8238.
26. Di Nardo JV. Biometric Technologies: Functionality, Emerging Trends, and Vulnerabilities. Journal of Applied Security Research. 2009;4(1-2):194-216.

27. Galbally J, Ross A, Gomez-Barrero M, Fierrez J, Ortega-Garcia J. From the Iriscode to the Iris: A New Vulnerability of Iris Recognition Systems. Black Hat USA; Las Vegas, NV; 2012.
28. Gelb A, Metz AD. Identification revolution: Can digital ID be harnessed for development? Washington, DC: Center for Global Development; 2018.
29. Quinn GW, Grother P, Matey J. IREX IX Part One. Performance of Iris Recognition Algorithms. NISTIR 8207. Maryland, USA: National Institute of Standards and Technology; 2018.
30. Uhl A, Wild P. Comparing verification performance of kids and adults for fingerprint, palmprint, hand-geometry and digitprint biometrics. IEEE 3rd International Conference on Biometrics: Theory, Applications, and Systems; Washington, DC; 2009.
31. DNA Helps Reunite Children With Their Families: Universidad de Granada; 5 August 2009 [Available from: https://canal.ugr.es/prensa-y-comunicacion/medios-digitales/medical-news-today-reino-unido/dna-helps-reunite-children-with-their-families-9/].
32. Basak P, De S, Agarwal M, Malhotra A, Vatsa M, Singh R. Multimodal biometric recognition for toddlers and pre-school children. IEEE International Joint Conference on Biometrics (IJCB); 1-4 Oct.; Denver, USA; 2017.
33. de Luis-Garcí a R, Alberola-López C, Aghzout O, Ruiz-Alzola J. Biometric identification systems. Signal Processing. 2003;83:2539-57.
34. The Engine Room, Oxfam. Biometrics in the Humanitarian Sector. Oxfam; 2018.
35. EU JRC. Fingerprint recognition for children. Report EUR 26193 EN. Italy: European Commission, Joint Research Centre; 2013.
36. Soutar C. Biometric technologies in support of identity and privacy assurance. Biometric Technology Today. 2011(November/December):5-9.
37. Buolamwini J, Gebru T. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. In: Sorelle AF, Christo W, editors. Proceedings of the 1st Conference on Fairness, Accountability and Transparency; Proceedings of Machine Learning Research: PMLR; 2018. p. 77--91.
38. Blanco-Gonzalo R, Lunerti C, Sanchez-Reillo R, Guest R. Biometrics: Accessibility challenge or opportunity? Plos One. 2018;13(3):e0194111.
39. Storisteanu DML, Norman TL, Grigore A, Norman TL. Biometric fingerprint system to enable rapid and accurate identification of beneficiaries. Global health, science and practice. 2015;3(1):135-7.
40. Storisteanu DML, Norman TL, Grigore A, Labrique AB. Can biometrics beat the developing world's challenges? Biometric Technology Today. 2016;Nov/Dec(11):5-9.
41. Choosang P, Vasupongayya S. Using fingerprints to identify personal health record users in an emergency situation. International Computer Science and Engineering Conference (ICSEC); 1-6 Nov.; Chiang Mai, Thailand: IEEE; 2015.
42. Koda Y, Higuchi T, Jain AK. Advances in Capturing Child Fingerprints: A High Resolution CMOS Image Sensor with SLDR Method. International Conference of the Biometrics Special Interest Group (BIOSIG); Darmstadt, Germany; 2016.
43. Liu I. Infant Footprint Recognition. IEEE International Conference on Computer Vision; 22-29 Oct.; Venice, Italy; 2017.
44. Jain AK, Cao K, Arora SS. Recognizing infants and toddlers using fingerprints: Increasing the vaccination coverage. IEEE International Joint Conference on Biometrics; Florida, USA; 2014.
45. USAID pilots biometrics to track youth health in Kenya: Planet Biometrics; 9 October 2015 [Available from: http://www.planetbiometrics.com/article-details/i/3620/desc/usaid-pilots-biometrics-to-track-youth-health-in-kenya/].
46. Iritech Inc. Biometrics for education [Available from: https://www.iritech.com/biometric-education-Kenya].
47. Biometrics an option for schools wanting a secure future. 14-19 Learning & Skills Bulletin. 2016(203):19.
48. Chinchilla R. Ethical and Social Consequences of Biometric Technologies in the US. Eastern Illinois University: American Society for Engineering Education; 2012.
49. Lodinová A. Application of biometrics as a means of refugee registration: focusing on UNHCR's strategy. Development, Environment and Foresight. 2016;2(2):91-100.
50. Gelb A, Mukherjee A, Navis K. Digital governance in developing countries: Beneficiary experience and perceptions of system reform in Rajasthan, India. Working Paper 489. Washington, DC: Center for Global Development; 2018.
51. Sharma V. AADHAAR- A unique identification number: Opportunities and challenges ahead. Research Cell: An International Journal of Engineering Sciences. 2011;4(Sept.):169-78.
52. Hosein G, Nyst C. Aiding surveillance. An exploration of how development and humanitarian aid initiatives are enabling surveillance in developing countries. Working Paper 2014/1. IDRC and UKAid; 2014.
53. Viola de Azevedo Cunha M. Child Privacy in the Age of Web 2.0 and 3.0: Challenges and Opportunities for Policy. Innocenti Discussion Paper 2017-03. Florence, Italy: UNICEF Office of Research- Innocenti; 2017.
54. Lalović K, Milosavljević M, Tot I, Maček N. Device for biometric verification of maternity. Serbian Journal of Electrical Engineering. 2015;12(3):293-302.
55. Weingaertner D, Bellon O, Silva L, N. L. Cat M. Newborn's Biometric Identification: Can it be done? Third International Conference on Computer Vision Theory and Applications; 2008.
56. Tesini DA. Development of a biometric infant identification tool: a new safeguard through innovation. International Journal of Childbirth Education. 2009;24(2):25-8.
57. Mayhew S. Mandatory fingerprinting of children in South Korea faces backlash: biometricupdate.com; 21 June 2018 [Available from: https://www.biometricupdate.com/201806/mandatory-fingerprinting-of-children-in-south-korea-faces-backlash].
58. Lihua Z. Iris recognition technology proves identities. China Daily. 17 November 2016.
59. Buolamwini J. Gender and skin-type bias found in face analysis systems. Biometric Technology Today. 2018;2018(3):2-3.
60. Aadhaar linked to half the reported starvation deaths since 2015, say researchers: Huffington Post; 26 September 2018 [Available from: https://www.huffingtonpost.in/2018/09/25/aadhaar-linked-to-half-the-reported-starvation-deaths-since-2015-say-researchers_a_23539768/].
61. Zelazny F. The Evolution of India's UID Program: Lessons Learned and Implications for Other Developing Countries. CGD Policy Paper 008. Washington, DC: Center for Global Development; 2012.
62. Dyer O. Police in Xinjiang province gather biometric data under guise of health programme. BMJ. 2017;359:j5865.
63. Alterman A. "A piece of yourself": Ethical issues in biometric identification. Ethics and Information Technology. 2003;5:139-50.
64. Hooper B. The case for better privacy standards. Cambridge, UK: Simprints; 2017.
65. Lyon D. BIOMETRICS, IDENTIFICATION AND SURVEILLANCE. 2008. p. 499-508.
66. Kish M. Nike's expanded effort to collect data from college athletes raises privacy concerns. Portland Business Journal. 16 September 2016.
67. Arnold JF, Sade RM. Wearable Technologies in Collegiate Sports: The Ethics of Collecting Biometric Data From Student-Athletes. American Journal of Bioethics. 2017;17(1):67-70.
68. Nyst C. Children and Digital Marketing: Rights, risks and opportunities. Geneva, Switzerland: UNICEF, Private Sector Engagement; 2018.
69. Danovaro-Holliday MC, Ortiz C, Cochi S, Ruiz-Matus C. Electronic immunization registries in Latin America: progress and lessons learned. Revista Panamericana de Salud Pública. 2014;35(5):453-7.
70. Guidance on collection and use of biometric data. In: Office of the Privacy Commissioner for Personal Data, editor. Hong Kong 2015.
71. Kuner C, Marelli M, editors. Handbook on data protection in humanitarian action. Geneva, Switzerland: International Committee of the Red Cross; 2017.
72. UNHCR. Guidance on the protection of personal data of persons of concern to UNHCR. Geneva, Switzerland: UNHCR, Division of International Protection; 2018.
73. Galbally J, Haraksim R, Beslay L. A Study of Age and Ageing in Fingerprint Biometrics. IEEE Transactions on Information Forensics and Security. 2018(99):1.
74. Baker SE, Bowyer KW, Flynn PJ, Phillips PJ. Template Ageing in Iris Biometrics. In: Bowyer KW, Burge MJ, editors. Handbook of Iris Recognition Second edition. London: Springer; 2016. p. 541-54.
75. Dinkar AD, Sambyal SS. Person identification in Ethnic Indian Goans using ear biometrics and neural networks. Forensic Science International. 2012;223(1-3):373.e1-13.
76. Fenker SP, Bowyer KW. Analysis of template aging in iris biometrics. IEEE Computer Society Biometrics Workshop; 17 June 2012.
77. Fairhurst MC. Ageing and biometrics: an introduction. In: Fairhurst MC, editor. Age factors in biometric processing. London: The Institution of Engineering and Technology; 2013. p. 3-16.
78. Lanitis A, Tsapatsoulis N, Maronidis A. Review of ageing with respect to biometrics and diverse modalities. In: Fairhurst MC, editor. Age factors in biometric processing. London: The Institute of Engineering and Technology; 2013. p. 17-36.
79. Wall KM, Kilembe W, Inambao M, Chen YN, Mchoongo M, Kimaru L, et al. Implementation of an electronic fingerprint-linked data collection system: a feasibility and acceptability study among Zambian female sex workers. Globalization and Health. 2015;11(1):27.
80. USAID. Identity in a digital age: Infrastructure for inclusive development. USAID, Team SR; 2017.
81. Rinaldi A. Biometrics' new identity—measuring more physical and biological traits. EMBO Reports Science & Society. 2016;17(1):22-6.
82. Berman G, De La Rosaii S, Accone T. Ethical Considerations When Using Geospatial Technologies for Evidence Generation. Florence: UNICEF Office of Research- Innocenti; 2018. Contract No.: Dissussion Paper 2018-02.
83. FindBiometrics. What are biometrics 2019 [Available from: https://findbiometrics.com/what-are-biometrics/.
84. Arutyunov VV, Natkin NS. Comparative analysis of biometric systems for information protection. Scientific and Technical Information Processing. 2010;37(2):87-93.
85. Kindt E. The Processing of Biometric Data. A comparative legal analysis with a focus on the proportionality principle and recommendations for a legal framework. Leuven: Katholieke Universiteit Leuven; 2012.
86. Stewart B. Privacy Impact Assessment Handbook. In: Commissioner OotP, editor. Auckland: Office of the Privacy Commissioner; 2007.
87. Gold S. Biometrics- a global review. Biometric Technology Today. 2011;April(4):5-8.
88. Tractica. Global biometrics market revenue to reach $15.1 billion by 2025. 6 February 2017 [Available from: https://www.tractica.com/newsroom/press-releases/global-biometrics-market-revenue-to-reach-15-1-billion-by-2025/].
89. Privacy International. Biometrics: Friend or foe of privacy? : Privacy International.

© UNICEF/Frank Dejongh

ANNEX I

Biometric project planning template

It is recommended that country teams complete at least the Background and Description sections prior to starting in order to help you work through the questions in this guidance. Don't worry if the document is not complete or you don't have all the answers as the text may need to be revised or updated as you progress. Once complete and you have worked through the flowchart questions in the guidance – you should have a project summary to assist you in moving forward to next steps if you have decided to proceed.

Background and Description of Project

CONTEXT

Country:	
Geographic location (national or describe):	
Sector:	
System manager (UNICEF/Partner/Ministry/etc.):	
UNICEF project manager and team:	
Brief purpose of the project:	
Is this a research project or pilot?	(If yes, you may need to complete a more thorough review before proceeding – see Section IV)
Describe the context in which you are working:	(Describe access to sites, security, internet coverage, literacy, political stability, etc.)
Describe the relevant legal instruments:	(Are there provisions in the country that may affect the system design and implementation, eg. authorising collection of personal data, privacy provisions, sharing of data with the government, etc).

SYSTEM

What biometric trait will be used?	
Does the system need to operate in identification mode?	(See Q4)
Do you have any information on the vendor and measures of system performance?	(If yes, attach performance documentation at the end of this outline)
Has this system been used elsewhere in similar circumstances?	(If yes- Describe)
Is this a new system, or is biometric technology being linked to an existing system?	(Describe)
If this is an existing system – how are people currently identified in the system?	
What other systems need to be able to share data with this system?	
Over what time period will the system need to operate?	
Is there a proposed system structure (data flow/ storage/ components etc)	If yes, please attach details.

SYSTEM USERS

Describe whose data will be included in the system:	(Include age, gender, other characteristics)
Will biometric traits be collected for children?	
How will they interact with the system?	
Is informed consent to be obtained:	(If yes, detail process for 'informed')
Are there vulnerable groups or specific populations that may require special attention in the project design or implementation?	If yes – please detail these

SYSTEM MANAGERS

Who will manage enrolment and collection of the data?

-What qualification or skills will they need?

Who will manage the data storage, access, systems, etc?

-What qualification or skills will they need?

Who will be able to access the data? Are different levels of access anticipated?

Will data be shared with external or third-party vendors?

Who is responsible for responding to or managing concerns, data breaches or complaints?

PROJECT ASSESSMENT

1. Does the use of biometric technology add value to the program? Yes / No

Explain:

2. Is there an established legal basis for collecting, receiving, or sharing biometric data? Yes / No

Explain:

3. Is the biometric technology appropriate for the target age group(s)? Yes / No

Explain:

4. Is the biometric technology accurate and reliable for the proposed project use? Yes / No

Explain:

6. How acceptable are biometrics among the target community? Yes / No

Explain:

7. Could the introduction of biometrics potentially exclude children or families from services or protection? Yes / No

Explain:

8. Can the data be appropriately protected at all stages from collection (or receipt) through to destruction? Yes / No

Explain:

9. Can data privacy and protection concerns be appropriately managed? Yes / No

Explain:

10. Are potential partners and implementing agencies equally committed to data protection and privacy measures? Yes / No

Explain:

DECISION

Is there sufficient justification to move forward to next steps (including an evaluation of the cost, feasibility, implementation, and governance issues)?	Yes/ No

Explain the basis of your decision

Date of the assessment:

Project members who completed the assessment

Name	Title	Signature

unicef

data for children