2 0 2 3

# A Responsible Development Biometric Deployment Handbook

Version: January 2023

www.simprints.com

simprints
every person counts

# Contents

2023

Acknowledgements — This handbook was authored by James Eaton-Lee at Simprints Technology Ltd, and generously supported by the Notre Dame-IBM Tech Ethics Lab, who funded work leading to this material. Such support does not constitute endorsement by the sponsor of the views expressed in this publication.

Thanks are warmly given to the team at Simprints who supported and provided invaluable input to this work, including Alexandra Grigore, Marissa Kim Nordentoft and Raghav Minocha.

Simprints also express their deep thanks and appreciation to the various KII respondents who provided input during the framing and design of this project, as well as other colleagues across the biometric and NGO ecosystem whose direct and indirect support & guidance was invaluable.

The handbook would not have been possible without the input and support of the steering committee, who provided invaluable input throughout the project, including both structured and unstructured review. Any errors or omissions in the final guidance remain wholly the responsibility of the author.

Steering Committee:

- Siobhan Green - IMC Worldwide
- Joshua Hovsha - Castlebridge
- Sam Jefferies - UNHCR
- Teresa Perosa - The Engine Room
- Ognen Plavevski - Catholic Relief Services
- Elizabeth Shaughnessy - Oxfam GB
- Sanjith Sundaram - MOSIP
- Quito Tsui - The Engine Room

# Introduction

Biometric data collection is becoming increasingly common in development contexts - achieving broad deployment in interventions operated by some of the world's largest humanitarian actors.

Deployments of biometric systems generally reinforce ***foundational*** or ***functional identity*** needs, those as defined by technology aimed at reliably identifying humans who are accessing or receiving services at various scales of implementation.

Robustly establishing and linking humans to data about them may have many benefits - including de-duplication, waste reduction, higher-quality data management, fraud deterrence or prevention, or integrations and referral between different systems.

Yet biometric deployment is far from without criticism - in particular for the **unmanaged risk of collecting and storing this data** - sometimes in specific instances, and sometimes suggesting the broad unmanageability of the risk a priori.

These risks are especially acute when working with vulnerable populations and in contexts with low or no civic understanding, legal framework, or other safeguards, and with scant regard for those benefits. Much commentary and policy focuses on these contexts and the implications when things go wrong[1].

Recent disclosures of the poorly-managed handling and collection of biometric data on vulnerable populations underscore that these are real risks - with life threatening impact[2].

These risks have been the subject not only of ongoing debate within the Development community's "Responsible Data" ecosystem, but also the specific target of campaigning and advocacy work & litigation where specific harms or shortcomings are alleged[3].

With regard to the risks and opportunities of biometric technology, as the drafters of this handbook, we recognise various things to be true:

1. That **biometric technology is likely to hold utility for *some* use-cases**. Its widespread use in consumer devices to aid safety and convenience, to aid in safe convictions in criminal justice, and continued exploration by humanitarian actors suggest that it has potential value to society and can be used in applications with both high social acceptance and which are in line with social ethics and the rule of law.

1 The Engine Room and Oxfam (2018) - Biometrics in the Humanitarian Sector
2 HRW (2022) - New Evidence that Biometric Data Systems Imperil Afghans
3 AccessNow (2022) - WhyID Campaign - Accessed at https://www.accessnow.org/whyid/

2. That **its inherent qualities** and **the discontent in civil society are also significant**, have too a basis in fact, and should be heard and respected. Biometric technology lends itself to applications which control, measure, and monitor. This leaves it open to error & misuse.

3. That at the time of writing, **a sufficient critical mass of robust practice - maximising the anticipated good whilst minimising harm - does not yet exist** in the humanitarian ecosystem to the extent needed to defensibly manage the inherent tension between these viewpoints.

4. That implementors will benefit from guidance on **how to deploy safely and respectfully** that considers risks and mitigating steps, but must remain ever mindful that **choosing to deploy is an ongoing and not a one-time decision** which should be continually reassessed on the risk of risk, capabilities, cost, and external factors. Any guidance must therefore be predicated on making these choices well.

It will be known by most readers that the law treats biometric data with caution, reflecting in particular point two.

Biometric data is recognised in Europe - alongside medical data and information on gender identity or race & ethnicity - as "Special Category", with the law reflecting explicitly that data *"particularly sensitive in relation to fundamental rights and freedoms merit specific protection"*[4].

The purpose of this guide is therefore best understood as ***exploring this specific protection*** with the humanitarian and development communities - and the tensions and challenges - especially in mind.

Our hope is that by extending and enlarging our clear concept of what ***the good*** looks like, it becomes clearer to attain for practitioners; the difficult questions easier to ask; and the good easier to signpost where absent.

In line with these principles we believe implementors should consider throughout their use of this and other guidance the **need to accountably protect data** (i.e. to protect data in a way which is structured and explainable), the **need to tailor safeguards and approaches to the context**, and above all to base their decision to implement (& safeguards) on **a genuine assessment of benefit to the affected population**.

To do this, we believe implementors must keep coming back to a fundamental guiding question, ready if the answers become 'no' to consider alternatives, whatever stage their work is at:

> **"Does this remain effective, safe, and necessary? Is there ongoing benefit to the people we're working with? Can I explain - and am I explaining - how and why?".**

Wherever you are in your adoption or exploration of biometric technology, we hope this guide gives you better tools to ask and answer these questions.

4 GDPR, Recital 51

# Structure and Usage

This handbook is intended for practitioners with some technical expertise in humanitarian or development technology, whose core role may be technology, policy, law, privacy, or a related field.

It is intended to give these consumers:

1. A **basic practical primer in the key concepts** necessary to make policy, purchasing, or program decisions regarding biometrics;

2. A **guide to selecting and implementing biometric tools** with a focus specifically on development and humanitarian applications;

3. A **set of risk management steps and guidelines** which enable accountable, risk-aware decision-making and deployment;

4. A **range of appendices which enable the embedding of this guidance and practice**.

It is not intended as a foundational guide to data, digital, or data protection (or as a deep foundational guide in biometrics). Whilst it makes reference to many data protection concepts, and will explain some, it makes no apology for omitting or glossing over some aspects of data protection and compliance which will be *important* for your use-case.

It must be augmented with foundational practice which can be gleaned from other guidance, including internal and external guidance on digital safeguarding, data protection, other aspects of law, ethics, and human rights theory.

If you are consuming this handbook as a relative newcomer to the world of biometrics, we suggest that consuming it sequentially (i.e. beginning with the Primer section before proceeding further) is likely to benefit you most.

Knowledge of the fundamentals - which will then allow you to build appropriate policy lines, processes, and make the right decisions for your organisation - is vital if you intend to make cost-effective, ethical use of biometrics[5].

Otherwise, if your organisation already has a policy framework, some capacity and skill, or have a specific need for subject matter guidance, you may choose to work through specific risk management sections, templates, or make use of the appendices directly.

5 Biometrics Institute (2020) The Three laws of Biometrics - Available At: https://www.biometricsinstitute.org/the-three-laws-of-biometrics/

simprints
every person counts

# Biometrics - a Primer

## Introduction

To understand how to implement biometrics responsibly, we must first have a basic understanding of biometrics with a focus on the aspects which matter when we make decisions about responsibility as a purchaser, implementor, or reviewer of institutional practice.

It makes sense then, first to ask the question - what are biometric systems? What do they do? And how do they differ from other systems with similar goals or which they integrate into?

### What are Biometric Systems?

Biometric Systems are processes, tools, and technologies which measure specific characteristics of human physiology or behaviour for the purposes of recognising or establishing the identity of specific, identifiable individual human beings[6].

Put more simply, they are generally digital systems which measure traits or characteristics such as movement, fingerprint or iris pattern which are unique. They do this to distinct individuals using hardware and software, and then capture this uniqueness in data structures - called ***templates*** which are stored and processed to make decisions about humans.

Templates, once produced, can be used to recognise that human again by comparing a subsequent sample or **probe** of the relevant trait with the stored template. Or if a previously stored template exists, the two can be cross-referenced and compared for likeness.

A biometric system will rarely exist in isolation. Typically it will be integrated into a broader IT Solution, perhaps collecting related data or linking a biometric record to an intervention or distribution activity - our treatment here of 'storage' suggesting already how a database of templates may be stored and used to identify humans.

### What are Identity Systems?

Frequently, a biometric factor will be captured as part of a broader ***Identity System*** which is established for the purposes of identifying humans across some timespan, geographic or jurisdictional boundary, or series of interventions.

Systems which are established for multiple ***purposes*** and applications are often referred to as ***Foundational Identity Systems***. For instance, since 1998 - when Malaysia introduced the first biometric passport - many countries have implemented or added  biometric factors which integrate into their issued passports, and which are stored in a backend passport database.

6 Biometrics Institute (2022) What is Biometrics? - Available At: https://www.biometricsinstitute.org/what-is-biometrics/

More recently, many governments have begun implementing digital identity systems at a national level which incorporate biometrics and are used to access government or social services such as India's Aadhaar System.

Foundational Identity is less common in the humanitarian ecosystem, where it is more typical to collect data for the purpose of a single program or intervention, or a limited collection of interventions carried out by a consortium or group of INGOs - for instance a cash consortium or multi-agency humanitarian response; or in settings where no foundational system yet exists.

These deployments are typically referred to as ***Functional Identity Systems*** **-** systems which, in effect, meet a *functional* need where more *foundational* systems do not exist, are unreliable, or cannot be used.

In any of these systems, the Biometric System itself may simply be a module in a broader foundational or functional system with no clear distinction for end-users - or even an entirely integrated component which passes data into the broader system.

## *Messy Edges*

At the boundary between Humanitarian and Development programming, where data collected for a short-term problem may be used over time and as the nature of a response becomes more long-term, this distinction may be malleable.

Data collected to enable an in-kind distribution of foodstuffs - a functional need - may be used two years later to invest in the longer term economic inclusion and wellbeing of a population who no longer need in-kind assistance but are rebuilding their lives - and could even over time begin to look more like a *foundational* platform serving a community who are long-term recipients of assistance.

In other instances - and increasingly common - NGO data collection happens in tandem with government systems, in particular where programming is longer-term (e.g. public health interventions). Some International Organisations such as the UN High Commissioner for Refugees (UNHCR) have mandates which explicitly include working with governments, and data may be collected with these government use-cases or dataflows explicitly in mind.

The boundary between functional and foundational ID is therefore not always clear, and can be highly political or funding-dependent; it may not be clear at the inception of project A that funding will later arise for project B, which gives rise to a bigger service opportunity.

The distinction however remains useful, important to understand, and relevant to planning and design as it has implications for privacy safeguards such as ***Transparency*** and ***Purpose Limitation*** which rely on anticipatory practices which consider (and communicate) likely use-cases - which we will touch on in the operational sections of this guidance.

### Biometric Concepts

However it is integrated or used, biometric systems will always be used as part of an interaction between an implementing organisation and an individual in the context of some intervention or assistance - it is improbable that collecting a biometric dataset is a final end in itself. These ultimate purposes are referred to in this guide as **service delivery**. But whatever the program, biometrics by necessity always involve people. Understanding how the technology is used then requires some root in language and terminology as it relates to them.

## People - Who's Involved?

The term typically used for the individual whose behaviour or physiology is being measured can vary from use-case to use-case; often it will mirror the broader intervention and a term such as "Service Recipient" or "Beneficiary" may be used depending upon the organisation.

But this guide largely uses the terminology adopted in the relevant ISO/IEC standard (ISO/IEC 2382-37:2017)[7] - where the human whose characteristics are being measured is referred to as the ***Biometric Data Subject*** (or simply ***Data Subject***, mirroring the term in Data Protection frameworks).

Other humans interacting with the equipment or software in **attended use-cases** - that is, use-cases where a 'supervising' human is present - are referred to as ***users*** or ***attendants***.

## Use-cases - What are they doing?

When this constellation of people work together, there are a few ways they are likely to do it. There are consequently four main 'use-cases' we will conceptually consider in this guidance, some or all of which may be present in specific program implementations.

The process of **enrolment** - initially registering a user on a biometric system- which will be present for most if not all humanitarian uses.

Once the enrolment process has produced an initial biometric record, the biometric data may be used in two key ways as part of service delivery:

A process of **Identification** - often referred to as 1:N or 1:Many Matching - in which a human is identified from a database or enrolled participants using the biometric data itself.

Differing subtly, a process of **Verification** - often referred to as 1:1 Matching - in which a hypothesis may exist regarding a human's identity (perhaps we know their name or they have presented an ID card) but we verify it against the stored record using biometrics.

7 ISO/IEC (2017) - ISO/IEC 2382-37:2017 Information technology - Vocabulary

Independently or in parallel, in particular where we have multiple datasets, we may use biometrics for **De-duplication** - taking the data and identifying & eliminating records where the same human is represented in multiple places.

We will step through each of these in turn to take the time to explore them better.

## Enrolment

In a typical deployment, an Attendant or User will initially carry out a process referred to as **enrolment** to register the subject into a biometric database at the beginning of the activity or endeavour - enabling the subsequent re-identification of the subject, for instance when they receive assistance.

As a specialist task with various failure modes and requiring distinct troubleshooting steps, this enrolment process should typically be carried out independently from service delivery or under closer supervision. It may involve collection of or cross-referencing against other data, such as name, government ID, temporary documents, and other demographic data.

## Identification

**Identification** operations are those in which the biometric data itself is used to identify a database entry or digital record relating to the individual. Identification is often the instinctive biometric use-case we may assume reflects a majority of usage - fed by Hollywood images of hands on glowing screens or experience with Law Enforcement use-cases involving facial recognition and surveillance tools.

**Warning** - Identification use-cases pose more hazard as the biometric system *itself* becomes responsible for an adjudication - or decision-making - step which relies on the matching process. As we will discuss later in this guide in considerations of accuracy, this can introduce greater chances of exclusion.

While the underlying technology may be virtually identical (a system deployed to do 1:1 matching may be easy to reuse for 1:N matching through reconfiguration), these nonetheless involve distinct processes and technology - in which the same operation is run multiple times and decisions are made primarily based on thresholds with no independent check such as the presentation of an ID document.

And in practice there may also be use-cases where 1:N matching is more dangerous - allowing a system built for a distribution to be used for surveillance or law enforcement - as well as opening more latitude for exclusion where the technology fails.

**Info** - 1**:** N matching systems with built-in enrolment may be our 'intuitive' sense of how biometrics work; for instance, surveillance systems in public places or as part of security applications often use sensors built into cameras which effectively enrol many subjects simultaneously. However, in practice due to accuracy, data collection, dignity, and other requirements many commercial and humanitarian applications can work a little differently depending upon the system and use-case.

### Verification

**Verification** operations primarily differ from identification operations in using some other means of initially identifying participants, such as scanning a card or keying in a username. In practice this mode is more common.

Where biometrics are attended, this verification stage is likely to happen in collaboration with the attendant, who may type in a name, read an ID number from a card, tap a smartcard on a reader, or even recognise the user from prior interactions.

In a Verification Operation, the biometric system is likely to be comparing the user to a much smaller pool of possible matches - perhaps 5 users with the identical name, or even 1 record if the user has presented a card or ID number - where an Identification may require comparison against hundreds or thousands of records.

This makes Verification faster and potentially higher accuracy as the biometric 'matching' process is run fewer times (potentially by orders of magnitude if the database held by the system contains thousands of records and must be searched through each time a 1:N match is made) and is not the only source of 'truth' for a judgement regarding whether the subject is the correct subject.
Where an operation returns multiple possible matches in a scenario with an attendant present - or the biometric system returns a confidence score (for instance, it indicates a probability onscreen that the user is who they say they are as a percentage or using language such as 'good/bad/poor'), the process of determining whether to proceed is referred to as **adjudication**.

## System Components

Now that we have some sense of who might be doing what, it's useful to understand what is under the lid; what happens when your finger touches the glass of a scanner or you're registered?

Biometric Systems themselves typically have a number of sub-components. Sometimes - for instance where a hardware device is used for capture - these may be physical subcomponents, or clear integrated tools visible in system architecture.

**Info -** Consider the systems now in use in some airports which allow electronic passport checking. In these systems the scanner is a physical unit which is clearly visible, often with a moving camera or sometimes a consumer webcam on a desk. In these instances, with a biometric passport, the 'data storage' is also separated - in your passport, as well as in the passport issuer's backend system.

Where a tool is largely implemented in software and pre-integrated - for instance, facial recognition tools which leverage built-in cameras provided by a single vendor - these may be so heavily-integrated that the boundaries are invisible to the user.

**Info -** Consider the fingerprint scanners or facial unlock features in use in most modern mobile phones - the sensor may be invisible or a general purpose component with multiple uses, and all of the subsequent system components integrated into the phone's software.

But even where a solution is largely implemented in software, they may have different origins - combining best-of-breed solutions from multiple vendors, or some Open Source and some proprietary components; they may even be on different sides of the planet where cloud tools are used.

Clearly, being able to break apart the components of a biometric system may be deeply necessary to understand and to evaluate how accurate, ethical, or safe it is.

The biometric component of a broader system will also generally not exist on its own; it will integrate with other data collection tools, identity systems, or potentially more exotic tools or data structures, such as distributed storage systems or cryptographic tools.

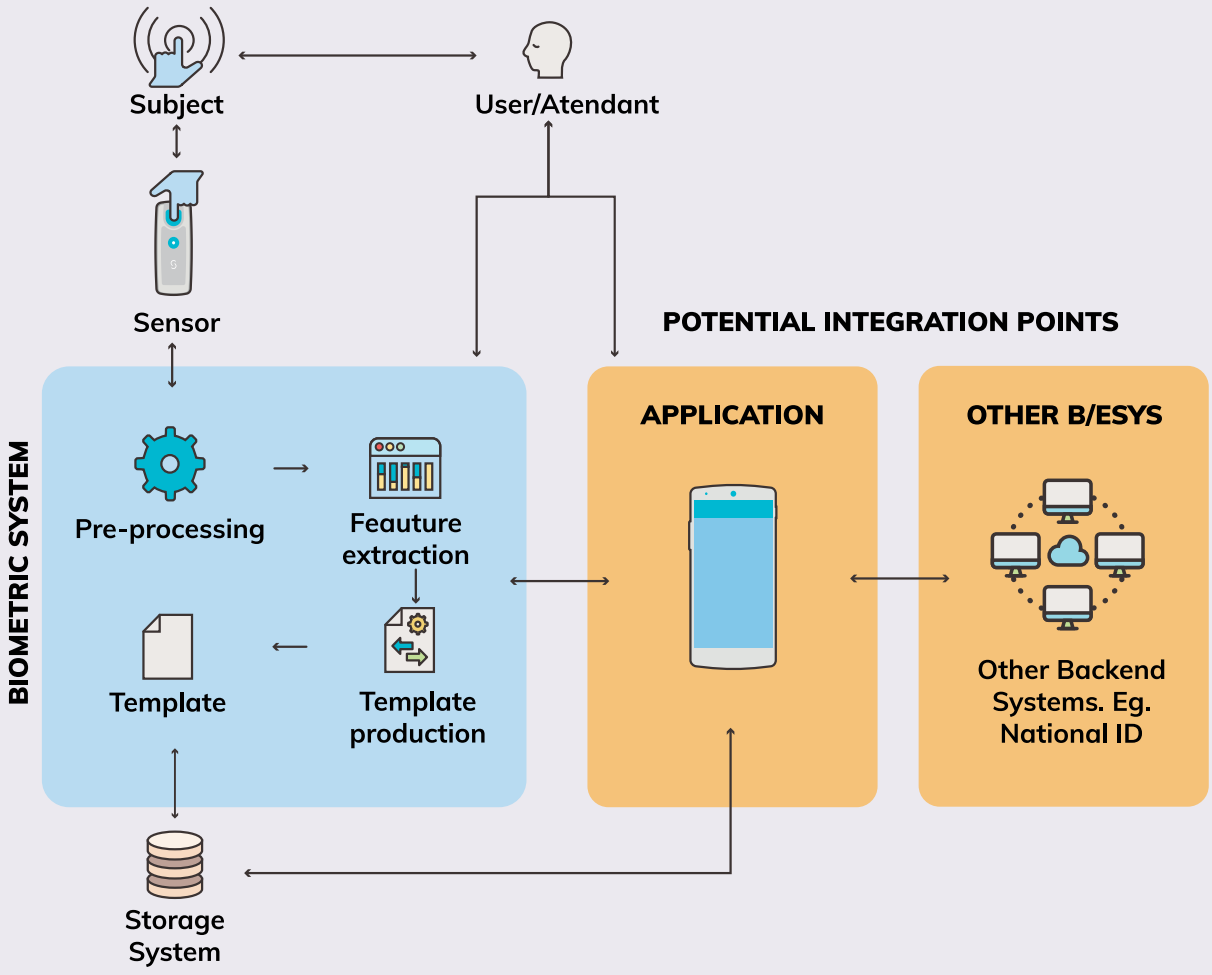



*Fig 1.*

Some understanding of this architecture is useful - as it will form the basis for both understanding and risk assessment when mapping the dataflow of a given system.

For the purposes of this guide, we break down the biometric system into the following components, using standard terminology which should match that used in ISO, academic, or other literature:

In hardware-based solutions which utilise a physical device for capture, the biometric workflow may begin with a **Sensor -** i.e. an electronic component which may use light or infra-red radiation to capture data from the subject.

The data captured by the sensor will then typically be handled by **Pre-Processing** technology. This might compensate for ambient light conditions, highlight specific areas of the physiological or behavioural aspect being measured, or otherwise optimise the data captured to maximise the changes of a successful extraction.

This data will then typically be handled by a **feature extractor**. This takes what may be referred to as 'raw data' - e.g. a picture of a face, fingerprint, or iris - and produces as an output a set of derived data which will typically be smaller in size - and reflect 'features' which are meaningful when carrying out operations such as matching.

**Info -** A helpful metaphor could be a comparison between an aerial photograph and annotations of specific map features of interest exist - including lists of roads or structures, but missing features the extractor deems irrelevant such as the type of crops in a field or existence of informal structures or paths. Feature extraction is the process of making this list of 'key features'.

One of the most well-established and understood forms of feature extraction is the production of "minutiae" from fingerprints, identifying where specific lines end, cross over, or where other features such as dots exist - the digital equivalent of traditional manual fingerprinting.
But there are many forms of feature extraction - including extraction of features in irises, the distance between facial features, etc, and leveraging various technical approaches.

## Templates

Once data is extracted, it will be assembled into a **template** - essentially the compilation of the list of features into a reusable 'map'.
Template generation can be relatively standardised (for instance, there is a standard, ISO/IEC 19794-2:2011, for minutiae-based fingerprint templates). But this varies by application - face and other modalities are less standardised. It is worth knowing too that some protective safeguards take effect by modifying the way the template is produced - covered in a later section.

Considering this analogy, we may intuit how some equity issues begin to be introduced in these system components- an extraction algorithm producing a map of formal roads might be excellent for some applications but fail when considering populations who use informal footpaths not reflected on the map.

Less metaphorically, consider how an extraction algorithm may fail in contexts it is not designed for, for instance with worn or scarred fingers, differing skin colour, or in sub-optimal conditions.

Traditional extraction methods such as minutiae-based fingerprint algorithm may allow evaluation of shortcomings - whilst extraction methods

which use Machine Learning (ML) and where the 'features' selected will not be known or understood may be more flexible if they are well-designed and trained - but also impossible to understand, as well as non-interoperable. Both have benefits and drawbacks which may apply differently in different contexts.

## Storage and Use

Once templates are produced, they will inevitably be stored and used in some application. There are various **ways to store templates** once produced - some applications may store them on a capture device such as a mobile phone, whilst others may immediately sync into the cloud, or store on a 'local factor' such as a smartcard held by the user.

Conceptually, where a number of templates are stored and used for comparison (e.g. a database of enrolled participants) this is often referred to as a **gallery**. This terminology is uncommon outside biometric subject matter experts.

Lastly, the most crucial component - the **application** itself. All of the components covered so far may be obscured as part of a biometric module, component, or integration - often separate from the business application using biometrics - perhaps a health application, cash distribution tool, or case management system.

How these integrations behave will vary - in some instances they may be tight, returning biometric data directly to the application and storing it alongside records of care or transactional records. However, especially where good practice is followed, there may be separation, whether in two databases or platforms, or a more distributed or unusual storage mechanism such as smartcards held by the subject or a distributed storage mechanism such as a blockchain or other data structure.

Naturally, how and where data is stored also has an influence in particular on the safety claims which can be made about it - different storage

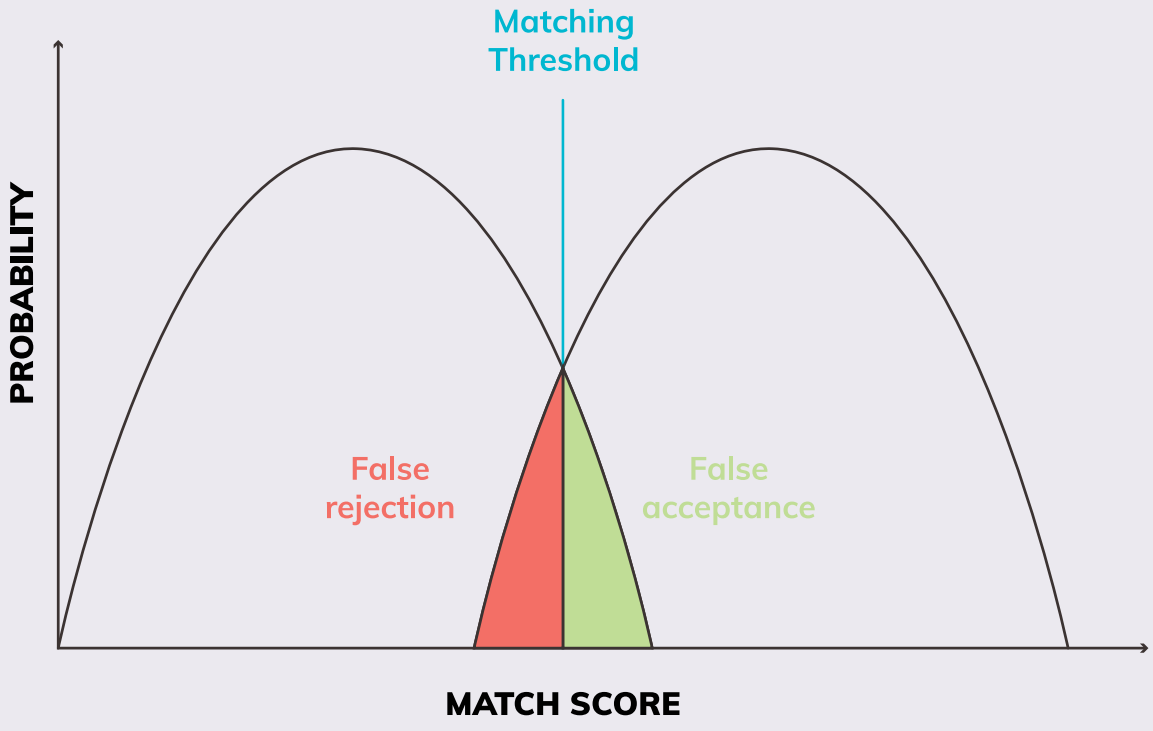



*Fig 2.*

locations will have different implications for theft, seizure, failure of security controls, or misuse. More considerations on the risk of these factors are given later in this document.

## Quality

### Biometric Accuracy

Accuracy of biometric data is a complex topic - where any reductive number, view, or principle should be treated with both excitement and deep suspicion.

It is also a topic of balance; balance between more accurate (but disproportionate) collection; between unachievable or unaffordable perfect accuracy and accuracy which is 'good enough' for the task; and an ultimate understanding of the accuracy of a specific intervention rooted in the underlying need and benefit, as well as the consequences of a failure to identify or verify specific participants.

There are various components of biometric systems - from the sensor to the matcher - whose behaviour and effectiveness may make "accuracy" better or worse. All of these components may be configurable, and the training of users & supervision will also affect their behaviour and outputs.

Even in a simple system, the question "how often will a distribution fail because a user is falsely rejected" can therefore be hard to answer without a deep understanding of the system in question and how it might perform.

Most biometric systems do not in fact operate - unlike other systems used for authentication such as passwords or cryptography - in a binary way.

The comparison done by a matcher between a template stored in a gallery and the biometric data provided by a user is instead likely to be scored, with a matching process using the outcome of this scoring process to make a decision.

The matching process is typically configured with a **threshold** value, correlating with a matching score chosen to find a balance between **false acceptance** - i.e. allowing a high number of subjects to match who are 'imposters' - and **false rejection** - i.e. preventing legitimate subjects from being recognised and potentially accessing services.

This process is inherently probabilistic. Once a matching threshold has been found for a specific population and intervention, it may remain relatively constant - but a threshold chosen for an intervention with a population in Europe may have significant difference in behaviour with a population with a substantially different ethnicity and skin colour; and an urban population of clerical workers may perform differently to a rural community whose hands may be worn.

Thresholds must be calibrated for specific populations, based on an understanding and appreciation that these probabilities are part of the 'business' of making binary judgements about fuzzy data.

**Warning** - Consider how your intervention might calibrate the threshold to the population as part of the project plan, and when it might need to be reassessed - and what this means for your procurement, partnership, and working pattern with technology providers.

There are a number of metrics frequently used to measure and understand the overall accuracy of a system, including whether the threshold

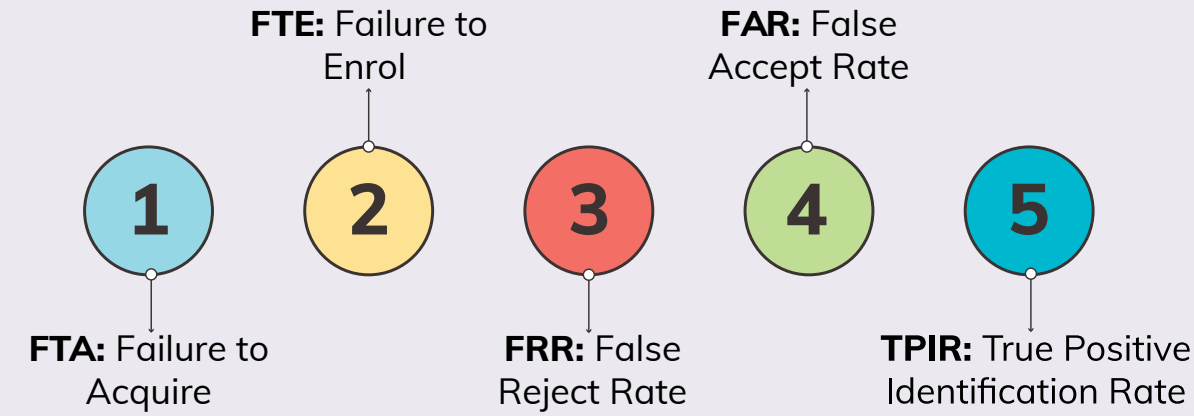



*Fig 3.*

is correctly set but also whether other system components are functioning correctly. The most common and useful are:

**Failure To Acquire (FTA)** - i.e. the failure of the device to acquire a biometric image;

**Failure To Enrol (FTE)** - i.e. the inability to enrol the subject into the system;

**False Rejection Rate (FRR)** - i.e. the proportion of genuine subjects who are turned away;
**False Acceptance Rate (FAR)** - i.e. the number of subjects who are accepted who should not have been;

**True Positive Identification Rate (TPIR)** - i.e. how often the correct subject is identified at the top of the list during a search.

There are many other measures - some specific to verification or identification operations - but knowledge of these five is likely to be sufficient for non-specialists.

FTA will typically occur in circumstances where there is a critical failure of the hardware, the environment, or the training of the user. A hardware platform not designed for the skin colour of participants, for the environmental conditions (e.g. humidity or warmth), hardware damage, or poor finger placement may all lead to FTA. Where FTA is high, programs are unlikely to be successful at all and end users may circumvent tools entirely.

FTE may occur where the hardware acquires an image, but it is of poor quality - perhaps still the result of poor hardware, but potentially also poor lighting or other environmental factors. It may also be indicative of low acceptance or attendance - perhaps where subjects are ill, refuse the solution, or the solution only works for a subset of the target population. Where FTE in particular is high, the likelihood of exclusion may be especially high, and projects may prove costly & slow.

FRR - perhaps the result of the same factors as a FTE, where enrolment may have happened in a control environment but subsequent use has been 'field-based', or where participants' circumstances may have changed - is also likely to pose a risk of exclusion, and may in a worst case produce unrest, deep mistrust, disadvantage and harm.

FAR (or in an Identification application, the related metric False Positive Identification Rate - FPIR) may indicate that the solution is more susceptible to fraud - or will have low acceptance by users, perhaps requiring significant amounts of manual adjudication or work to find the right participant.

As we discussed earlier, FRR and FAR will never be zero, but sustaining a managed balance will be the goal for most programs; if either is too high, the solution will pose risks to implementation.

For most programs, the TPIR will be the one simple number to monitor - i.e. the frequency with which the correct individual is identified first time round. Like FAR, if the solution does not do this frequently, or significant manual adjudication and searching is required, the solution at best may be expensive and ineffective, and at worst actively harmful.

**Warning** - Consider when planning projects which accuracy measurements are most useful to you, and when selecting solutions which you may need the solution to provide. Be wary of "baserate" figures from manufacturers which are not supported by evidence or context - how solutions perform in the lab and in the field can be very different.

## General Data Quality Issues

So far we have talked mostly about quality and accuracy as it relates to the capture of biometric data itself.

We have also introduced concepts relating to the use of the system - in particular reflecting that biometrics may be attended - i.e. a user supervises the subject during capture. Here there will also be quality factors which arise from their use of the system; in particular where **adjudication** is performed by the user, who may need to select from a list of likely or possible matches during an identification event.

Here, to be fair and accurate, not only will a system need to be technically accurate, but its use must also be fair and the user appropriately trained.

A second consideration is data biometric data is linked to, and the role of the biometric data in this broader dataset. Biometric data is rarely if ever captured by itself; it will invariably be captured and linked to some other record - perhaps a healthcare or transaction record. This data itself will have its own quality and accuracy considerations.

Here, biometric data is frequently used to enhance quality in particular by identifying **duplicate records** in a process often referred to as **de-duplication**.

De-duplication is possible because one biometric dataset may be compared against another, or a registration or enrolment against the database it relates more broadly to, allowing a user or system to answer two key questions using an aspect of the subject's physiology:

1. Could this user be the same as one of my previously-registered service recipients?
2. Does this user exist in other databases?

The second use-case - i.e. comparison - is in some ways the most challenging; data may not be interoperable between different systems, comparison naturally requires some exchange of data, and this usage is most likely to be a secondary use-case which could be intrusive, excessive, or unethical.

However, there will be use-cases such as healthcare where cross-referencing records may have lifesaving or beneficial consequences.

De-duplication is likely to happen in two places:

1. At enrolment - i.e. by performing an Identification event *on the existing database* prior to enrolling the participant.

   This may not be possible in instances where the full database is not available to the user, but is generally the simplest and most effective solution where the goal is simply record management and duplication avoidance.

2. As a backend process - working on the data itself in the backend.

This may use the biometric data alone - e.g. by comparing records against each other and calculating which records have the highest match scores. But in practice, this process is likely to require manual intervention - or adjudication - either to ensure high quality or add a manual step[8] in which a human reviews these scores and makes a manual or semi-manual determination.

Where manual or semi-manual de-duplication is performed, it is likely not just to involve the biometric data, but also the demographic data. For instance, matches with >90% confidence may independently be compared to identify instances of similar names, regions, customer profiles, or other data which allow a high-confidence decision to be made. This is particularly likely to be the case where false de-duplication (e.g. merging health records) is high-impact.

**Warning** - If your project needs de-duplication, consider what you will need to do to support it - both in terms of functional requirements of the tech, but also the overall dataflow - will you need, for instance, to supplement a deduplication process with other data - and whether this is compatible with the purpose the data was collected for, and your broader understanding of the risk.

## Types of Biometric System

### Other Features

Besides De-duplication, there are many other features of biometric systems which may be functional add-ons or specific capabilities that are valuable - and have a bearing on responsibility.

Much of this guidance focuses on attended biometrics - where a staff member, volunteer, or community member is operating equipment during the course of a program. But in some cases, a subject may also be the user - i.e. the individual whose biometric is being taken will be operating the equipment themselves.

This is the case where we use biometrics to access our phones, or in some cases where we access services remotely, such as via apps which remotely verify identity to allow remote enrolment to government services.

In these cases, a user cannot be relied on to thwart obvious attempts to circumvent biometrics - such as a user holding up a magazine page instead of putting their face in front of a scanner, or placing a prosthetic finger on a scanner.

Some solutions offer technology for **liveness detection** - e.g. asking the user to move their head while presenting their face - or **anti-spoofing** - e.g. resistance against prosthetic finger biometrics for these use-cases.

While not always relevant for humanitarian or development action - which will often be attended - this functionality will increasingly be relevant where assistance is delivered remotely, especially with no end in sight to movement and travel restrictions as the result of global public health crises.

Similarly, many well-established modalities of biometrics such as fingerprint rely on contact or physical proximity to operate effectively. Some solutions - such as facial recognition, or phone camera-based palm or fingerprint recognition - offer **contactless** capability, reducing the risk of disease transmission and potentially increasing throughput.

8 Article 22 of the GDPR, for instance, mandates a manual decision-making process where this type of Automated Decision-Making process is carried out in some circumstances, and so it is likely to be necessary as an optional workflow even if not used in 100% of instances.

Many of these technologies are in their infancy - with active research ongoing in areas such as contactless palm vein and palm biometrics. But longer-term applications designed for a wide audience will want to keep tracking market behaviour as these technologies become widespread.

**Warning** - at the 'cutting edge' they may remain significantly more expensive than solutions based on ubiquitous consumer hardware such as face or specialised hardware with "paid-off" Research and Development costs such as fingerprint readers. Contactless solutions such as Palm Vein, while promising, are likely to remain high-cost for humanitarian and development actors for some time.

## Modalities (& Hardware)

There are many biometric modalities. The most common are face, fingerprint, and iris; measuring characteristics of the layout of the face, ridges and patterns on the finger bed, and patterning and colours of the eye.

But these are only a handful of approaches available, which include voice recognition, movement, measurement of veins below the surface of the skin, geometry of the whole hand, and various others. Many products even implement "multi-modal" biometrics, which incorporate multiple methods into one identification or verification flow.

Each has benefits and drawbacks - in particular:

- Where the **state of the art** is; some are better developed or understood than others, with greater or lesser market maturity, availability of support and tools; the benefits here may be subtle and include differences not only in market availability but also accuracy and quality.
- Whether **hardware is required** and as a corollary, how expensive (or effective) the solution may be in a given application.
- Restrictions such as **age range** the modality works across, **environmental limitations** such as dust, moisture, or working environment requirements.
- **Data** and **Interoperability** - for instance, whether the modality benefits from enough standardisation that templates may be reusable with other systems.
- General **intrusiveness and reusability** - some modalities such as face may be inherently less pseudonymous when data is captured, whilst others such as vein may produce data which is both less tightly decoupled to the user's personhood and identity, but also more medically intrusive and which potentially discloses other aspects of the user.
- **Social acceptance** - which will naturally vary by context. In some settings, facial recognition may be unremarkable, whilst in others it will be hugely inappropriate.
- **Contact/Contactless** - some solutions will not be possible to use at a distance. Whilst this can be a privacy benefit (reducing the likelihood of covert sensing), this may also pose public health challenges.

No solution will be right for every application, but the section below outlines some general considerations which practitioners may use to shape their exploration, drawing from various sources as well as the experience of the author[9][10]. The choice of modality will be context and agency-specific, but these resources should be used as a starting point.

9 Biometrics Institute (2018) - Considerations for Implementing a Biometric System
10 World Bank (2022) - A Primer on Biometrics for ID Systems

| Modality | Notes | Ubiquity / Maturity | Drawbacks | Benefits |
|---|---|---|---|---|
| Face | **Facial recognition typically measures geometry and relationship of facial features.** | Widely implemented and understood in commercial applications, with a variety of consumer and other applications.<br><br>Relatively well understood, and widely deployed for law enforcement and other applications. | Overlaps with Law Enforcement and may make Facial Recognition challenging to obtain acceptance for in some settings.<br><br>In cultures in which facial covering has a cultural or religious aspect, facial recognition may not be appropriate, and introduce gendered challenges both in terms of user and subject.<br><br>Most conducive to 'trivial' reuse - e.g. users may immediately be able to reuse pictures of users to recognise or identify them.<br><br>While a robust understanding of accuracy exists in the academic community, and issues of bias are relatively well understood, they are not always solved or resolved. | Contactless - posing fewest public health challenges (e.g. transmission of surface or airborne disease).<br><br>No specialist hardware required, making facial recognition relatively cost-effective.<br><br>While Liveness Detection is not embedded into all solutions it is widely available.<br><br>Some protective techniques such as tokenisation or encryption are available to protect facial templates. |
| Fingerprint | **Fingerprint recognition is essentially a digital analogue of the analogue process undertaken in law enforcement, using the scientifically established near-uniqueness of fingerprint features to identify humans.** | Widely implemented and understood in commercial applications, with historic usage across law enforcement and security applications.<br><br>ISO standardised, making some Fingerprint templates interoperable between solutions. | The overlap with law enforcement may make fingerprint systems less acceptable in some contexts.<br><br>Most fingerprint systems require specialist hardware, increasing cost.<br><br>Generally contact-based, increasing the risk of surface-borne disease.<br><br>Some user training is required to use hardware effectively.<br><br>May not work with seriously physically impaired subjects. | Significant understanding exists regarding bias and accuracy, and whilst skin colour can be a confounding factor, the use of hardware which controls the capture environment offers some ability to mitigate this.<br><br>Of available solutions, fingerprint may be the most interoperable.<br><br>Fingerprint recognition also benefits from some of the most sophisticated techniques for template protection and encryption.<br><br>Fingerprint recognition captures relatively little 'extraneous' information (e.g. medical conditions etc) once the template has been captured.<br><br>Whilst not unspoofable, the need for specialist hardware makes replay or spoofing attacks harder to carry out, increasing resistance to fraud. |

| | | | | |
|---|---|---|---|---|
| Palm Geometry | **Palm Geometry techniques measure the shape and size of fingers using camera or similar technology.** | Less common, but a number of solutions are available. Palm geometry has been in use in the private sector (e.g. banking) for some time. | Less interoperable and understood.<br><br>Historically, this has required specialist hardware, although can now be undertaken via camera / with commodity hardware.<br><br>Fewer techniques available for sophisticated protection e.g. using template protection or tokenisation schemes. | Relatively high social acceptance - captures minimal 'extraneous' information such as medical conditions.<br><br>Contactless - posing fewest public health challenges (e.g. transmission of surface or airborne disease).<br><br>No specialist hardware required, making facial recognition relatively cost-effective.<br><br>Palm geometry captures relatively little 'extraneous' information (e.g. medical conditions etc) once the template has been captured. |
| Iris | **Iris recognition techniques measure the eye itself, recording and comparing unique features in the iris.** | Less common, but subject to some large-scale deployment in humanitarian settings.<br><br>Iris recognition has been deployed in the private sector (e.g. banking) for some time. | Less interoperable and understood.<br><br>Historically, this has required specialist hardware, and specific capture conditions - and requires proximity to capture, increasing cost and complexity at point of use.<br><br>May not work with seriously physically impaired subjects or individuals subject to eye surgery.<br><br>Affected by lighting change, and requires configuration and supervision.<br><br>Less inherently resistant to spoofing / impersonation attacks.<br><br>Some protective techniques such as tokenisation or encryption are available to protect facial templates - but fewer than fingerprint or face. | Relatively high social acceptance - captures some 'extraneous' information such as medical conditions, but less than other modalities.<br><br>Like fingerprint, while not 100% unique, Iris patterning is extremely random and determined prior to birth, potentially giving rise to a very low false match rate.<br><br>While proximity is required, Iris is less 'high contact' than modalities such as fingerprint, posing reduced disease transmission risk.<br><br>Works with cohorts of users who use facial coverings.<br><br>The Iris is protected and less susceptible to damage than finger or hand. |

| | | | | |
|---|---|---|---|---|
| Periocular | **The capture of the area around the eye, including eyebrow and other facial features above the mouth.** | Less common; some recent research, but relatively few commercial products. | Less interoperable and understood.<br><br>May be confused by users with facial recognition.<br><br>Fewer techniques available for sophisticated protection e.g. using template protection or tokenisation schemes. | May leverage consumer hardware and therefore reduce cost.<br><br>Higher social acceptance than full-face.<br><br>Contactless - reducing surface-based transmission risk.<br><br>May combine with Iris recognition to produce some of the benefits of both systems. |
| Palm vein | **The capture of the sub-surface veins in hands, typically using infra-red light and a specialist sensor.** | Some recent research but less common. Fewer commercial products but a number of actively innovating projects and vendors. | Less interoperable and understood.<br><br>Requires specialist hardware - increasing cost and reducing interoperability.<br><br>Still in active innovation - subject to change over time.<br><br>Fewer techniques available for sophisticated protection e.g. using template protection or tokenisation schemes. | High social acceptance.<br><br>Some medical data is captured, but relatively little extraneous data (e.g. facial image) which can trivially be reused.<br><br>Contactless - reducing surface-based transmission risk.<br><br>Vein patterns are relatively unaffected by age, disease, or physical damage, increasing accuracy over time. |
| Voice Recognition | **The capture of the voice using an audio sensor.** | Relatively wide use, but fewer products targeting users in the Global South. | Less interoperable.<br><br>May be more susceptible to confounding accuracy factors with populations with languages and dialects who solutions have not been designed for.<br><br>Fewer techniques available for sophisticated protection e.g. using template protection or tokenisation schemes. | Higher social acceptance than other solutions.<br><br>Relatively no extraneous data is captured.<br><br>Contactless - eliminating surface or airborne transmission risk.<br><br>Leverages widely available commercial hardware. |
| Multimodal | **The combination of multiple techniques or modalities** | Less widely deployed, but a number of products are integrating multimodal support. There are some systems at large scale using multi-modal biometrics. | Depends on the schemes used. | Depends on the schemes used - but potentially multimodal biometrics presents the opportunity to combine and trade benefits and disadvantages of multiple schemes. |

## Templates & Biometric Storage

We have discussed throughout this guidance already the typical storage process for biometric data once produced - the use of templates.

It is by no means guaranteed that biometric data will be stored in a template - 'raw data' can be stored and rarely may be an appropriate form of data capture. In some instances, a structure more sophisticated than a template may also be used. In this section we explore these types of storage.

### Raw Data

Rarely, raw data from the biometric probe may be stored beyond the 'ephemeral' storage of this data in the memory of a hardware device or general purpose computing device necessary to run an extraction algorithm or other process.

Storing raw data for general use in matching or verification is discouraged by most good practice guides on safety. Raw data carries no privacy safeguards. It is often trivially easy to 'reassociate' with the subject (a face image will, for instance, be immediately recognisable as the image of the subject), and it is likely to store significant extraneous information - such as clothing worn by the subject, medical conditions, environmental conditions, and potentially even location or other data.

For general purpose deployment it is unlikely ever to be "the right choice" for these reasons to store raw data or source images.

Implementors may consider storing raw data in some circumstances - in particular where:

- Deployments have **research aims that relate to biometric accuracy** and require raw data to evaluate components of the system - for instance, comparing different template generation or feature extraction algorithm;
- Long-term deployments using proprietary algorithms need **to cater for a change of technology or vendor by regenerating templates** in a 'new' incompatible or proprietary template format in circumstances where re-enrolment is cost-prohibitive but a more accurate, cost-effective, safer, or competitive product exists;
- Systems use **different/incompatible template formats but still have de-duplication requirements;**
- To support **long-term transfer of data** - for instance from a functional into a foundational system which may use an unknown template format.

These circumstances are unusual - most humanitarian use-cases will not have these requirements. But in particular where innovating or working over longer timeframes or in close proximity to government or other partners, raw data could be the right choice.

Where raw data is stored, the processing activity may incur the risk factors mentioned above. However, some mitigating factors may exist. Raw data, for instance, which is stored for "long term" compatibility with future vendors or government foundational systems may **be able to store raw data in a secure vault** or in cryptographically protected cloud systems which offer significantly more protection than 'operational' template data which is disbursed or accessible. The use of techniques such as key escrow or offline storage will further enhance the protection offered by such storage.

Implementors who feel raw data is right for them will need to:

1. Be clear in their analysis that the opportunities offered by raw storage are appropriate and proportionate to the project aims;
2. Identify appropriate privacy safeguards such as appropriate levels of subject consent, ethical research approval, enhanced consultation and transparency;
3. Identify appropriate technical safeguards when holding the data which are linked to the underlying threat model such as cryptography, offline storage, and siloing;
4. Ensure the safeguards, opportunities, and risks are clearly balanced and reevaluated.

These safeguards are not explored in this document in depth and are likely to require specialist support; organisations choosing to store raw images should ensure they have the right budget, capabilities, and tools to undertake this work.

**Warning** - For most deployments, storing 'raw' or source images will introduce significant and potentially unmanageable risk. If you are considering doing this, ensure that assessing the need/benefit of raw storage is explicitly a part of your design process, supported by the right skills and budget, and that you identify appropriate safeguards for this higher risk storage choice.

## Template Storage

Biometric data once captured is typically stored in a template. Templates are produced by an 'extraction algorithm' and subsequent generation process, condensing key features from the data initially captured into a data pattern which is then 'representative' of features in the biometric factor which should not change.

Traditionally, systems have been engineered and may work in a similar fashion to 'human' recognition - for instance, fingerprint algorithms are often 'minutiae-based', recognising key features of the human fingerprint such as specific line shapes, where lines fork or combine - and representing these distinct 'minutiae' as a pattern a little like the map of a town or village.

Newer systems which use Machine Learning or other systems may use other approaches, potentially offering no 'understandable' rationale for storing specific features or datapoints but nonetheless using the same fundamental principle - i.e. that key features or properties that should not change will be captured in the template.

Templates are sometimes advocated as 'safer' than raw images. This is to a certain extent true. In particular, a template:

- Will for a casual human be difficult to reidentify without other data or the user present (a user cannot, for instance, look at a face template and recognise it to a human);
- Will be less likely to store extraneous information such as medical conditions, environmental circumstances, etc.

Nonetheless, templates are not in and of themselves a protective scheme and should not be thought of as 'equivalent' to encryption or other schemes. They are at best an encoding scheme - i.e. a manner of data storage with some properties and reduction in overall data, but which nonetheless **are** biometric data - otherwise they would not have utility.

## Privacy Preserving and Alternative Storage Technologies

Templates can, however, be supplemented by additional protection. There are a range of Privacy-Preserving Technologies and safeguards which offer to reduce the risk associated with storing templates - including **Traditional** or **Homomorphic Encryption,** which may protect the data for some portions of its journey or keep it 'unreadable' for certain processing activities.

While homomorphic encryption may for some deployments offer privacy safeguards, 'Traditional' Encryption (*i.e. 'at rest' and 'in transit' encryption using public key or other encryption designed to prevent interception attacks or extraction of data from systems which can be directly accessed by an attacker who has compromised them*) may offer limited privacy protection when data in use.

This is because with traditional cryptography, data will need to be read - and therefore decrypted - when it is used, weakening protection potentially for the majority of the data's "life" in live systems, as well as introducing a new challenge (protecting the key used to carry out the encryption process). More analysis is provided in Data is Data is Data.

While (other than traditional encryption at rest) these techniques remain in 'early adoption' for most vendors and implementors, **Biometric Template Protection** and other approaches such as **Tokenisation** are available for some vendors, and the subject of considerable research and analysis, including for humanitarian use[11]. Some humanitarian actors have begun to explore and codify the use of these and other technologies in their policies[12][13] but in spite of established research, the risk reduction they offer, and some technological availability they are not yet widely deployed, prompting even the concern of supranational regulators[14].

### *Tokenisation*

**Tokenisation** is an approach to data storage which replaces a record with a 'token' that has less sensitivity - and which could be lost or stolen without incurring harm or compliance impact. Tokens are typically a random or substituted value - which when working with biometrics, a token should lack the properties that make a biometric template risky - for instance the linkability back to a human.

Tokenisation is widely adopted in some fields including card payments, where it has been adopted for several years[15] to mitigate the risk associated with storing information which is desirable to an attacker and can easily be stolen or inadvertently disclosed.

**Biometric tokenisation** is also possible - and widely used in some consumer applications. A biometric token may store 'alternative' data such as a pointer back to a record stored elsewhere, or authentication data allowing a receiving system to know that a suitable identification, verification, or other security event has taken place without processing biometric data.

Tokenisation has been adopted by some large-scale development applications, and can be cheaper & easier to implement than encryption

11 Sukaitis, Justinas (2021) - Building a path towards responsible use of Biometrics
12 ICRC (2019) - The Policy on the Processing of Biometric Data
13 Oxfam (2020) - Biometric and Foundational Identity Policy
14 Wojciech Wiewiórowski (2020) - The State of Biometrics; an update from the European Data Protection Supervisor - Accessed at https://edps.europa.eu/sites/edp/files/publication/20-10-07_edps_biometrics_speech_en.pdf
15 PCI SSC (2011) - PCI DSS Tokenization Guidelines

technology[16], but will be reliant on support by biometric and other software tools.

### *Template Protection*

Sitting in between outright replacement with a token and 'pure' storage (whether encrypted or not) sit **Biometric Template Protection (BTP)** schemes which attempt to address the shortcomings of template-based storage by adding (or removing) properties from the stored template which render the data less inherently harmful when released.

Template Protection schemes are defined in an ISO Standard - ISO 24745 - but various other approaches exist, including technology which 'locks' the biometric data to a user's biometric data (preventing user without the presence of the user) such as **biometric cryptsystems**, **biohashing** and various other techniques.

While this is a broad and complex field, implementors will find it useful to understand the key properties which Template Protection schemes attempt to provide and which are not present when biometric data is stored in a plain template:

**Irreversibility** - i.e. the inability to reverse a template in order to extract data about the subject, such as an image of the face or other data about a finger, eye, or other body part or behavioural aspect.

Template protected templates, when irreversible, should not permit an attacker with access to a template to 'see who a user is' without using other (i.e. biographic data) and should reduce the ability to infer or extract extraneous information such as the presence of physical damage to the face or finger.

'Ordinary' templates, if stolen, would allow a motivated attacker to extract 'raw' data from the template, picturing a user, obtaining additional information about them, and more effectively linking 'stolen' or leaked data back to the user, and thereby repurposing, misusing, or profiting from the stolen data.

**Unlinkability** - i.e. the inability to compare templates taken from the same subject to each other.

Template protected templates, when unlinkable, should not be compared across systems - i.e. if Agency A and Agency B both enrolled the same human (S), it should not be possible for an attacker with access to the stolen databases A and B to establish that S is enrolled in both. This should therefore reduce the linkability of the user and therefore other harms such as targeting, identity theft, crime, or abuse as a result of lost or stolen data.

'Ordinary' templates, if stolen, would allow an attacker to compare stolen data easily with other systems using the same technology, and link a user or identify them across multiple systems, establishing for instance that a humanitarian aid recipient was the same individual as in a government or other database.

**Renewability/Revocability** - i.e. that when templates are created from a subject, they are independent and separate.

Template protected templates, when renewable, should be re-issuable, enabling a distribution or financial system to use a 'fresh' template if its backend is compromised which does not allow an intruder with stolen template material to impersonate the user using that material. While

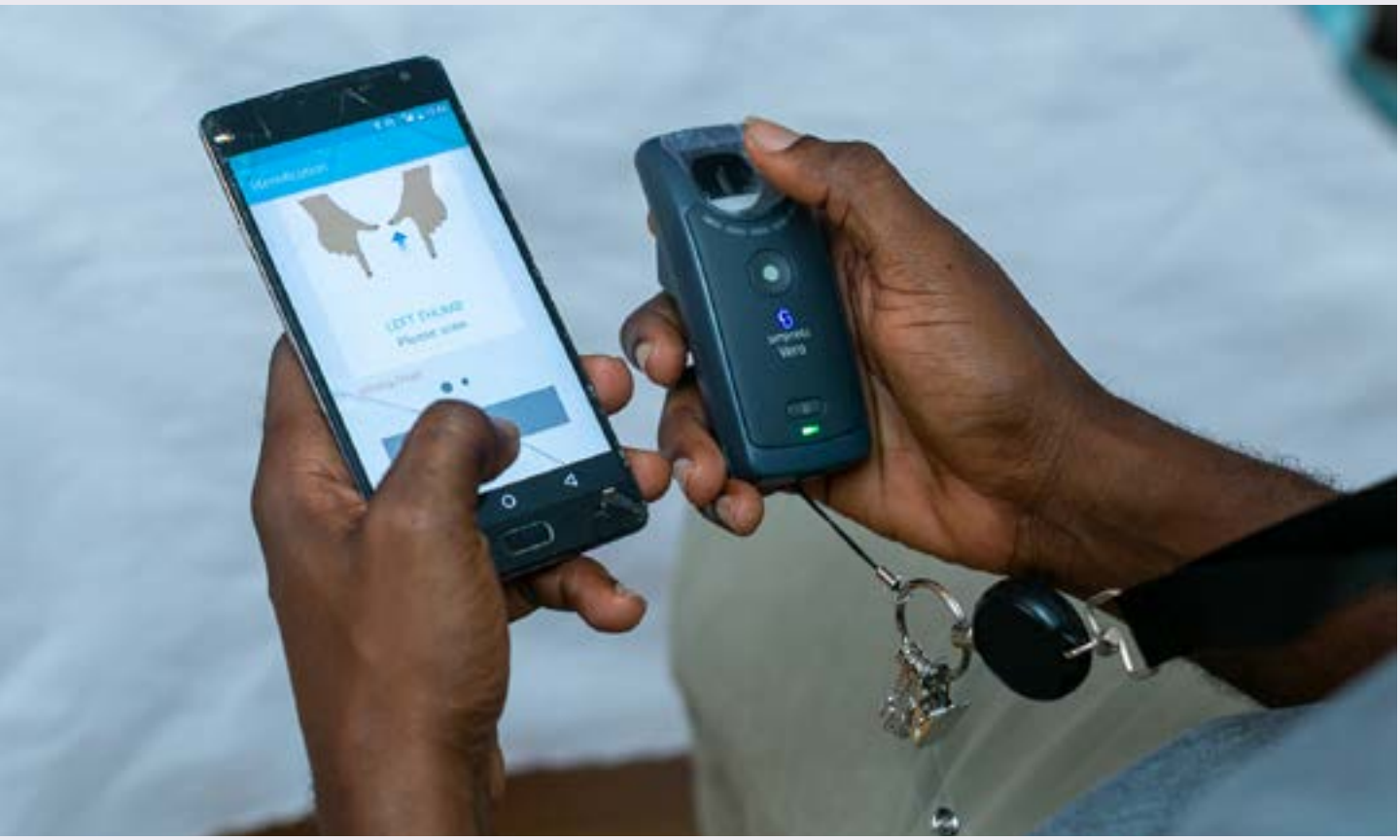
16 World Bank - ID4D Practitioner's Guide - Accessed at https://id4d.worldbank.org/guide/tokenization on 1/12/2022

the attacker might be able to use the stolen material to identify the user, a renewable (or **cancellable**) template will protect the system making use of the biometric from certain types of fraud or misuse.

'Ordinary' templates, if stolen, may be reused by the attacker to access systems in some instances and there would be no simple way for the system to identify or negate this misuse.

These properties will be seen in some instances to have immediate utility in a humanitarian context in limiting in particular reuse of data - the property of **unlinkability** in particular may address harms arising from theft and misuse, significantly reducing the ability of a state actor to seize humanitarian data and 'reuse' it in conjunction with its own data to target humanitarian service recipients.

Yet none is perfect, all have limitations, and there will be implementation challenges - BTP templates may be hard to deduplicate, less interoperable, or supported by fewer systems. Implementors must make their own evaluation of which schemes are available and appropriate for them, but are strongly encouraged to explore and evaluate these and related technologies for higher risk use-cases and complex threat models.



# Risk Assessment & Threat Modeling

Much of this guidance so far has treated foundational concepts and issues, suggesting equity issues or safety challenges that might arise from particular features, components, or design decisions but not in the context of any model or methodology for incorporating this learning and practice in design.

While this foundational knowledge is vital, modern approaches to Privacy, Security, and Data Ethics typically emphasise “by design” incorporation of learning and understanding - often using “method engineering” or similar anticipatory approaches which aim to incorporate characteristics, requirements, and themes into the design and construction of information systems.

There are many such approaches to ‘By Design’ incorporation of privacy and security approaches into digital systems, and various related families of technique such as value and human-centric design which may supplement or form the basis for them.

For the purposes of this guidance, we will consider three - overlapping - techniques and processes which we suggest most biometric implementors will wish to have some familiarity with and which should form the basis of any responsible implementation - providing frameworks for harnessing the knowledge, specific risk factors, and types of analysis the guidance suggests into artefacts and processes which are of practical use to implementors as they navigate their work.

## Risk Assessment

The first is the venerable **risk assessment.** Risk assessments - ‘paper’ analysis driven by a methodical understanding of the potential areas within a project which could give rise to unexpected outcomes, cost, or other harmful impact to the project goals, stakeholders, funders, and subjects - should be a core part of any implementation or procurement cycle.

Organisations may choose to incorporate risk assessments in a variety of places, but they should begin by defining the assets, project, or problem space the assessment relates to. This might be broad - for instance, a platform being acquired for a variety of specific projects, or a country in which solutions might be implemented. Or it may be narrow - a specific project or opportunity involving a small group of stakeholders.

Defining the scope and extent clearly allows you to identify what limitations the assessment might have, compile the right background material, and consult the right stakeholders. It may be self-evident - but sometimes has elusive, disputed, yet fruitful border areas.

Based on the scope, a responsible risk assessment will generally work through a library of potential failure points or adverse outcomes, considering factors which could cause the outcome to actualise, and which steps in the implementation

- or externalities to the project such as the behaviour of a partner, environmental change, societal factors, or conflict - which may produce or exacerbate them.

This stage of a risk assessment is often iterative - involving multiple rounds of re-assessment, stakeholder consultation, and scoring. It may harness a practitioner's innate understanding, the wisdom of a group, risk libraries or discussion groups. There are many methodologies for undertaking this process.

However it is undertaken, the final outcome of a risk assessment will generally be:

- An overview of the scope, methodology used to identify risks, and any limitations;
- An overview of any relevant context, such as a description of the project or dataflow;
- A list of risks, outlining
  - the circumstances which produce the risk;
  - the consequences of the risk materialising;
  - typically including a scoring method, such as Impact & Probability (more complex scoring systems may accommodate impact factors or attempt qualitative measurement);
  - A recommended or agreed mitigation for the risks.

In a responsible project or endeavour, the risk assessment will not end with the production of a report; the outcomes will be assigned to owners, and a review cycle or governance framework for following up will be defined.

Most organisations will incorporate risk assessment into business processes, and many will have processes or approaches for undertaking them or business-specific methods for scoring and governance.

It may also be iterative - a risk assessment may begin during procurement and grow, evolve, and be updated as a project comes to fruition. There is no right or wrong way - provided that the outcome ('safe project') is met.

For the purposes of humanitarian implementors, we suggest that responsible procurement and implementation should consider incorporating structured risk assessment into the following lifecycle elements:

1. **The procurement process** for a solution - in particular where implementors such as humanitarian implementors maintain a 'portfolio' of tools designed to be rapidly deployed in response to crises. Risk assessments undertaken as part of the procurement process should particularly consider:

   a. The partner relationship where relevant with the tool provider, including commercial aspects of the relationship in line with good procurement practice;
   b. Technical aspects of the tool, including any appropriate technical safeguards, and the responsibilities of both parties during maintenance, use, and in the event of a critical data incident;
   c. Other technology and technical issues, such as data backup, integration with other tools, support, and longer-term compatibility or other technology risks;
   d. Which use-cases the tool is suitable for, including any limitations or risk areas which may require particular treatment during deployment.

2. **Specific funding relationships or other high-level partnerships**, such as consortia or innovation partnerships. Whilst risk

assessment is often left to 'implementation', key decisions and expectations regarding how data and digital systems are used are often made in the early stages of partnership, and organisations may wish to consider either beginning risk assessment steps here which are carried through to implementation, or incorporating in the assessment of the opportunity considerations around data, digital systems, and technology.

3. **The decision to deploy the tool in a specific circumstance and the design & implementation of the opportunity.** "Implementation" is often the space in which deep risk assessment is undertaken - and it is important. But organisations may wish to consider:

   a. Integrating 'implementation' risk assessment with earlier stages of partnership (2) or;
   b. Dovetailing this risk assessment with parameters set out when tools or platforms are built;
   c. Integrating digital and data elements into other risk assessment which is undertaken as part of rollout, including:
      i. Protection or Safeguarding risk assessment;
      ii. Security Management Plans or other Physical Security risk work;
      iii. Conflict or Context assessment;

Wherever risk assessment is integrated (and whether it is undertaken as an integrated exercise or separately), it is critical that:

   a. The overall dataflow of a solution or partnership is mapped out and considered at some point prior to 'go live';
   b. Structured consideration is given to "what might happen" at each stage of a system or partnership in the event of failures of people, process, or technology;
   c. This consideration involves the right stakeholders from technology teams, partner organisations, program teams, and other thematic risk specialists;
   d. The right elements of context are mapped and considered as part of the risk assessment - including people, geography, culture, and government;
   e. The assessment includes mitigations which are owned, governed, and followed up upon.

## Digging Deeper

Risk assessment often asks the question "What might go wrong?" - but the method used to answer this question is sometimes left to hurried stakeholder meetings or deskwork by staff with conflicting and competing priorities.

This challenge - of how to answer the question well - is a familiar one in the cybersecurity industry, which has battled for years to understand the behaviour not only of complex systems whose components and internal architecture are greater than any one human may be able to understand, but also exist as part of a hostile and adversarial problem space in which motivated attackers and adversaries seek to disrupt and damage those systems.

In response to the persistent failure to architect solutions capable of prevailing in this game of cat and mouse - the limitations of traditional forms of risk assessment, the security industry has begun adapting *anticipatory* practices which engineer-in structured thinking about "what might go wrong" - the best known of which is a family of approaches called **Threat Modeling**.

Conventional Information Security practice typically thinks of Risks as the combination of Vulnerabilities in assets - i.e. the presence of a weakness such as an easily-pickable lock or a weak software component - and a Threat - i.e. the existence of a human who might want to pick the lock, or the prevalence of lockpicking or burglary in the neighbourhood the lock is in.

One approach to Threat Modeling attempts to model and map these complexities systematically, allowing engineers to define a criteria for "when I have asked all of the right questions", but moreover to communicate what their product has been built to defend against.

Threat modeling in this form often leverages Data Flow Diagrams (DFDs) - logical diagrams breaking down systems into components about which the right questions can be asked - sometimes using frameworks such as STRIDE or LINDDUN, taxonomies of types of privacy and security weakness.

Other approaches include **Attack** or **Threat Trees** - ways to model consequences which are similar to other systems modeling or method engineering techniques.

And - particularly in humanitarian environments in which parties to a conflict are known and populations may be vulnerable to specific knowable threats (such as violence or physical harm), defining or identifying **attacker archetypes** - the likely range of agents likely to attempt to obtain data or breach systems - and their capabilities and competence - will help supplement 'systems-based' approaches such as dataflow or tree-based approaches and deepen the answer to the question "What might go wrong".

These approaches can be powerful ways to augment or underpin a broader risk assessment - in particular one which is intended to give input to diagnostic engineering, technology, or configuration steps.

No one approach will be right for any given application, but even a simple half-page outline of "who and what we think we are defending against " can elevate a risk assessment, and for humanitarian implementors, deeper systems-based approaches which integrate with Physical Security Risk Management processes and other risk thematics are likely to be necessary to truly be responsible.

## Privacy Impact Assessment

Finally, for many organisations, the entry point or culmination of risk-based work - in particular on specific projects - will be a **Privacy Impact Assessment (PIA)**- sometimes also referred to as a **Data Protection Impact Assessment (DPIA)**.

In many organisations this may be the only risk assessment which is undertaken, or potentially a focal point or supplement to other risk-based work.

Various national frameworks have introduced PIAs as a requirement in Data Protection legislation - notably the GDPR, which in 2018 mandated this form of structured risk assessment for European organisations in specific circumstances. But PIAs have existed in the canon of 'good practice' in the broader privacy space for some time, and are required by other national and other frameworks - including in US Federal law, which defines PIAs in a subtle different way to the GDPR.
For the purposes of this guidance, we are largely adopting a 'GDPR-like' sense of what a PIA should do. In particular, in understanding that a PIA - whether it meets the requirements of the GDPR

or aligned frameworks, or broader good ethical & privacy impact thought, should:

1. Map the **dataflow** of the in-scope intervention, including system interactions, data exchange with partners and subcontractors;
2. Understand the **Proportionality** and **Necessity** of the usage of the data (*we will add - with a root in the benefit to the Subject*);
3. Identify any risks to the Subjects whose data are being used in the course of these dataflows, mitigations to these risks, and assess the residual risk (*we have already suggested some parameters for doing this well*).

While not explicitly called out in statute, good practice - and the regulatory guidance from European Regulators - as well as the pre-requisites of "identifying risks" tends also to include other elements, such as:

1. An **assessment of the 'Lawful Basis'** - i.e. the pathway in law justifying the collection of data;
2. An **assessment of any other legal requirements** - e.g. legal requirements in the humanitarian operating context;
3. An **assessment of the context of the subjects** (in particular to understand the risks which might come to pass, and their **comprehension of privacy notices or other communications** with them);
4. Outcome of any **consultation carried out** - in particular for complex, contentious, or intrusive projects of public interest or concern;
5. **Broader assessment against Data Protection** or other principles - including good data lifecycle practice, including retention, sharing, and disposal.

Those familiar with the GDPR will know that 'privacy risk' is defined in law extremely broadly - considering not just data-related risk, but many forms of "*physical, material or non-material damage*", including *"significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data"*[17].

We may then consider 'privacy risk' in the context of a piece of Humanitarian programming involving social protection, not to begin or end at 'loss of data', but to include a subject's potential loss of employment, receipt of benefits, distress if data is shared, loss of control over future financial decisions or labour rights.

Viewed in this way, it should be clear that PIAs are an extremely broad instrument which may overlap with or complement other forms of risk assessment and responsible humanitarianism.

## In the Final Analysis

Organisations must make their own decisions regarding where and when risk assessment should be undertaken for them, in terms of their ethos, values, structure, capacity, and the specifics of the programming they are undertaking.

This may include heavily Data Protection-inspired approaches which draw heavily on the intersectional approach of the PIA, include various complementary or in parallel approaches, integrate more deeply into more traditional humanitarian roles and processes - or neither.

17 GDPR, Recital 75

**Warning** - Consider which steps are right for your organization and how to incorporate them - as well as what institutional, regional, or technical policies might be necessary to govern your implementation and signoff.

However organisations may choose to do it, we suggest that:

- Any tools adopted by organisations should not only be considered as 'technical assets' which are reviewed by IT or Security teams, but also abstract patterns for programming, and where the type and risks of the use of the tool are risk assessed when adding the tool to the organisation's toolbox, considering where necessary:

  - limitations on the use of the tool
  - capacity and training needs, and
  - offloading work from implementors &
  - arming them with guidance on implementation wherever possible;

- Funding and other partnership relationships should incorporate treatment of data and digital components, ensuring in particular that:

  - Roles and Responsibilities of parties are clear;
  - Objectives which are explicitly or implicitly likely to give rise to data collection, use, or exchange are identified and;
  - Any necessary discussions about sunsetting of tools, data sharing, long-term support, incident management, or ongoing needs for risk management are aligned upon;
  - That sufficient funding and consideration is given to doing this safely;

- Implementations themselves should incorporate into their design and implementation iterative risk assessment treating:

  - The proportionality and necessity of the usage of data;
  - Dataflow and exchange with partners;
  - The individuals affected by programming and their communities, including the benefit to them of the use of data and where possible consultation steps;
  - The context those individuals exist within, in the broadest sense possible;
  - The risks involved - including who is responsible and with a framework in place for regular review.

However organisations choose to do this, remaining sections of this document treat many of the risk areas unique to biometrics - and which analysis, thought, decision-making, and risk assessment will want to consider as it unfolds.

# Risk Factors and Suitability - Pre-Deployment

No one tool will solve every problem. It is therefore stating the obvious to say that Biometrics may not be the right solution to *your* problem. Where it is, there may be contextual factors which will need to influence your deployment to use it well or effectively; these may be trivial, or fundamentally affect your budget.

Like any technology - in particular one that carries cost and risk - ***matching the tool and the challenge*** is critical for several reasons:

1. Investing in the wrong tool may simply be a waste of time and money - diverting funds from interventions or activities which have more benefit to your organization or constituents;
2. Mis-matched expectations about effectiveness or utility may adversely impact your program - potentially reducing its quality and negatively impacting its participants;
3. In the worst case, failing to assess whether your tools are the right ones may result in data collection or use which is extractive, excessive, disrespectful, and indefensible.

Frequently, the question "is this the right tool?" is concealed by strategy, donor policy, available funding, or prior procurement decision. It can even become an undesirable question when technology choice is a sunken cost or relational issue.

But wherever you ask this question - it is likely in fact that you ask it in multiple places - it is **critical** to ensuring you avoid the misgivings listed above. You may answer this question as part of policy discussions or risk assessments; you are likely to iterate it as your program and work evolves; and you should be asking and answering it in consultation with the subjects whose data you work with.

To help you approach this broad question - as well as leading into deployment considerations - we suggest breaking the problem down essentially into three subsidiary questions:

1. Are biometrics the right fit for the functional requirement?
2. What does the context mean for our deployment, what risks does it introduce, and can we mitigate them?
3. Who are the people, how vulnerable they, what risks do the demographic of our participants introduce, and can we mitigate them?

**Warning** - We suggest that you should have an answer to each of these subsidiary questions in order to ask the broader one. If the answer to any of them is "no", "we don't know", or "we can't know" - this may be a trigger for you to consider an alternative.

## Need/Benefit & Use-Cases

A key component to the first question outlined above - Are Biometrics the right fit? - is understanding the need or requirements of the project, and being clear what the benefits of the technology being deployed actually are.

**Info** - This suggests an approach which you may undertake independently (as a planning tool), iteratively (as you progress through your project and the design evolves), or as part of a broader Risk Assessment (e.g. within a PIA or Protection risk assessment).

To undertake this, we suggest the following five key steps:

1. Write down and be clear **what the 'need' is** - in particular:

    a. **What are the functional and non-functional requirements of the project?**
    For instance, *functional* requirements may be specific features that the project team need to implement in order to meet a programmatic aim, integrate with another tool, or collect data that works for a specific purpose. These may be indirectly related to biometric data collection ('accurately link vaccine record to individuals' or 'prevent fraud'), or highly-coupled ('de-duplicate the patient recordset using fingerprint').

    Where requirements are specific ('..using..' or '..with..' language which specifies a method can be a giveaway) it can be useful to ask 'why' questions to be clear whether something is truly a well-defined requirement or is rather a non-functional requirement.

    *Non-Functional* requirements are often constraints or quality requirements - for instance, a need that must be met in a particular way, a safety constraint, or legal boundary.

    b. **What are the expected benefits of the project - and to whom?**
    Requirements are often benefits in disguise; we generally do not need to prevent fraud simply because we dislike it - it rather ensures that donors' funds have their utility maximised or service recipients do not lose in-kind goods.

    Recording benefits and being clear who receives them helps to balance cost, risk, and impact - and what might need to support or evidence them.

2. Consider whether there are **confounding factors** which may impact the benefit, in particular:

    a. **Perception** of risks - whether or not they exist;
    b. **Socio-cultural factors** such as acceptance of the factor;
    c. Whether the participants belong to a **marginalised group** or **other specific demographic** (such as age, race, ethnicity, key population member);
    d. **Whether the project is in fact sufficiently funded** to meet these goals - in particular, 'bad digital' where the goals are not supported by a robust technology stack or the right capacity/capability or the project may not be sustainable ater initial funding expires;
    e. **Other external factors** such as environment, conflict, or funding;

3. Consider the **Activities and Outputs which realise the benefits** and ensure the requirements are met.

4. **Consider and record the outcomes** these produce which lead to the benefits, and how are we measuring them.

5. Finally, **evaluate whether the confounding factors and risks outweigh the benefits**, and ask whether the collection of data is truly justified. Use your conclusion to guide your decision to deploy - and the next stages of the project, including risk assessments and sensitisation activity.

### Purpose

Once we know these aspects of our project, we can also articulate or begin to understand the **Purpose** or multiple purposes for the data we are working with.

The **purpose** of data collection links closely to the principle of **purpose limitation**, an important privacy safeguard which exists in many data protection frameworks. Some of these - including the GDPR - require assessment of the Purpose as part of the governance of any project.

The principle of **purpose limitation** is a privacy safeguard that explicitly blocks function creep where secondary project goals are not compatible with the original intent.

By being clear about the purpose from the beginning of a project, aligning it with a clear assessment of benefit/need, and being able to explain it to subjects, we underpin our intervention with fundamental clarity, reduce the risk of function creep, and maximise our broader chances of success.
Being clear about purpose early on may reduce the impact of unexpected change later in the project - ensuring we do not fail to consider other use-cases such as MEAL, data sharing with partners, or secondary use-cases which may otherwise cause significant impact to project goals.

A template designed to allow recording of these - and alignment with outcomes, monitoring, and the **Purpose** of data collection is given in Appendix - Template for need/benefit analysis.

An additional Appendix, Appendix - Biometric benefit analysis and maximisation - excerpted from the CovidAction-funded "Using Biometrics to fight Covid-19" paper, provides a starting point for kickstarting this analysis.

Once you have recorded these, you can then *balance the anticipated needs/benefits with the risks anticipated and the impact to individuals* - allowing you to provide a clear, communicable, and accountable picture of the intended and expected outcomes, as well as how you intend to resource them.

**Warning** - Consider how you evaluate and record these early in your project - and which assumptions, expectations, or guiding principles might need to be recorded as part of your needs/benefits analysis. Considering these 'hidden assumptions' and recording them well can be hard but extremely valuable.

## Assessing the context

It will be clear already that the context is intimately linked to understanding and maximising benefits of the project as well as understanding and managing the risk - not to mention right-sizing program design.

In whichever place (or places) context is understood and assessed, it must be understood and assessed in detail in order to ensure that these components of responsible program design can be properly exercised.

Context in particular is likely to affect three sorts of risk:

1. The approach we use to **communicate what we are doing** and **build social consensus** , remain accountable, or gather consent from the subjects or affected community;

2. Our ability to ensure we respect the **purpose limitation** principle - and the likelihood of externalities to our project resulting in reuse or misuse of data such as government requirements or requests for data;

3. The likelihood of breaches of **Confidentiality** - for instance as the result of context-based threat actors, breaches, or security incidents.

In many organizations, there will be well-established practices for context and conflict assessment, particularly in teams with deep humanitarian experience. But these processes may not consider the digital ecosystem, or cyber threats.

**Info** - Where your organisation already has context assessment processes, consider mainstreaming digital and cybersecurity themes into them.

In this section, we break key contextual elements down into the following themes:

- People - who are we working with, and how does it inform how we work with them?
- History & Culture - what is the experience and identity of the broader population(s)?
- People and Biometrics - and what if might pose specific challenges with biometrics?
- Conflict - specific factors likely to amplify risk
- Digital Ecosystem - what is the broader environment in which tech is used?
- Partnership(s) - who are the other entities involved?
- Consultation and Civil Society - who should we be talking to and hearing from?

## People

Who are the people you are working with? If your intervention relates to one country, there are some aspects which may be universal to the group you are working with - for instance, they may speak a common language or group of languages. The language and literacy of the population will have a significant impact on comprehension and understanding.

This will affect your design of consent processes as well as who you choose to engage with the population. Signage, helpdesks, enumerators, and other communication material will all need to be considerate of the languages spoken by the population, as well as the literacy and expected education level.

Where the group you are working with vary, you may also need to provide for adaptive approaches - making material available in different ways to different groups, or providing interpreters and manned helpdesks as well as using paper forms or digital tools.

Where your tools are digital, you will also need

to consider digital literacy as well as access to smartphones or other technology - particularly if any part of your solution (and risk management!) involve self-service (e.g. to check a balance, raise a query, or express a concern).
Often, these issues can be gendered, or affected by intersectional inequality - what other demographic differences might exist which your program will need to cater for - for instance, affecting some marginalised groups, age groups, or regions you are working in?

**Warning** - These factors of comprehension, power, access, and equity will have a deep effect on how you plan your consent, communication, helpdesk sites, distribution points and design your data collection. Ensure you factor in any risks presented by or to specific factors or demographics.

Finally, even where a group is relatively homogenous and able to actively participate in written-form communications or benefit from informed consent processes, it is vital to consider the power dynamic at field level - between providers and service recipients, institutions and individuals. This might include attitudes towards gender roles, caregivers, government and society which affect decision-making and comprehension.

## History & Culture

Beyond the individual, it is also important to understand the experience of the broader population. Where a group has experienced oppression or mistreatment - in particular involving or facilitated by the misuse of data or the exercise of power to oppress and marginalise - i.e. behaviours of groups which may map onto use of data by other groups - this may have deep and long lasting effects on expectations and attitudes towards data collection.

Similarly, the broader history of civil rights alongside expectations and power dynamics such as relationships of the individual with institutions, service providers, and caregivers - as well as expectations around communication style, directness, individualism / collectivism - will all play a part in influencing how a group will respond to an activity.

**Info** - The most effective way to understand and accommodate these factors is of course to involve the affected community in the design of the intervention, iterating and responding based on the testing and rollout.

Some groups will also have specific attitudes - cultural or religious - towards specific parts of the body which are more or less acceptable to show or share; the acceptability of taking pictures at all; the handling of pictures of children, women, the elderly, or the deceased; as well as the identity of attendants.

While lived experience of oppression or forcible data collection will clearly have an effect on attitudes, so too may denial of identity - creating artificial positivity towards initial enrolment. And even 'benign but poor' digital projects may have had an effect - in a context with a history of mediocre digital data collection, or failed rollouts, attitudes and perceptions may vary too.

**Warning** - Failing to consider these factors may result in low acceptance and high rejection of a solution which is traumatising or insensitive. This may also not be immediate - as or if cultural and broader political factors change attitudes towards compulsory registration or data collection may also change. In these worst cases, failing to learn from the context could result in active harm if a poorly-considered solution is rolled out.

## People and Biometrics

Beyond general considerations of risk and explainability, there are some factors which may present specific challenges to biometric data capture. These may either be homogenous across a population - an intervention targeting infant vaccinations may exclusively target underage participants - but for a broader intervention more care may be needed to identify specific demographics of participants where an intervention may pose more risk or be less effective.

| Factor | Risks | Potential Mitigations |
|---|---|---|
| **Participants below the age of majority** | **Transparency -** Underage participants are unlikely to be able to provide consent for an intervention. | Interventions may need to rely on parental or guardian consent - creating additional complexity during implementation.<br><br>Over a long program lifespan, it may be necessary to plan to refresh this consent if participants come of age. |
| | **Acquisition & Effectiveness -** Some biometric factors change over time - in particular during early adulthood.<br><br>While fingerprints or iris patterning may be a priori the same, the templates generated during early childhood may be sufficiently dissimilar later in life to present challenges to verification - or equipment may be incapable of operating with infants or children. | Carefully consider and test the effectiveness of tools for the population - and at the ages - affected by the intervention.<br><br>Consider carefully whether re-enrolment needs to occur over a longer program lifespan.<br><br>Ensure technology partners have experience working with cohorts similar to this one and can provide the right level of assurance and support. |
| **Culture/Gender** | **Gendered Acceptance -** the choice of modality may not be acceptable based on socio-cultural norms, or may require distinct adjustment such as self-administration, same-sex attendants, etc.<br><br>This includes where facial covering is common and removal or photographing or capturing imagery is less acceptable. | Carefully select and test the biometric modality with a pilot group before scaling up to rollout, and where socio-cultural issues are flagged as a potential confounding factor.<br><br>Consider disaggregating analysis by gender or other distinct cohorts to enable analysis of needs and acceptability in particular in contexts which are more socially conservative. |
| | **Cultural Acceptance** - in some cultures, capturing facial likeness or portions of the body may be taboo, less acceptable, or unfamiliar.<br><br>This may include unexpected factors - such as the use of glyphs or colors in user interfaces, on hardware, or the way lighting and capture equipment work, which have 'hidden' cultural context and may be meaningless or alarming in other contexts and present inclusion, acceptance, or simply effectiveness challenges. | Carefully select and test the biometric modality with a pilot group before scaling up to rollout, and where socio-cultural issues are flagged as a potential confounding factor.<br><br>Consider as part of testing understanding, hardware, culture, consultation with groups and key demographics. |

| | | |
|---|---|---|
| **Disability, Impairment, and other physical factors** | **Failure to Acquire / False Rejection** - with populations who suffer from disability or impairment, or have specific medical conditions - for instance damage to eyes or hands from conflict, illness, or manual work, leprosy or skin ailment, albinism or other factors leading to unplanned-for skin colouring - the biometric factor may be less reliable. | Carefully select and test the biometric modality with a pilot group before scaling up to rollout.<br><br>During selection, ensure the tools have been designed with these contextual factors in mind.<br><br>Ensure that adequate workflow & capacity exist to troubleshoot and respond on the ground. |
| | **Failure to Acquire / Inclusion** - with populations who suffer from significant disability - such as loss of digits or limbs - or where damage to the biometric factor is a significant concern (for instance in populations where a significant proportion of the population have damage to the fingerpad or eyes) biometrics may consistently prevent enrolment or present inclusion issues. | Carefully select and test the biometric modality with a pilot group before scaling up to rollout.<br><br>During selection, ensure the tools have been designed with these contextual factors in mind.<br><br>Consider alternatives to biometrics and/or ensure robust monitoring is in place for inclusion and disadvantage.<br><br>Ensure that adequate workflow & capacity exist to troubleshoot and respond on the ground. |
| **History of 'Bad Data' or Marginalised Groups** | **Acceptance** - where a population has a history of data misuse or oppression, participants may find data use hard to understand or traumatising. | Carefully research the history of data, and consider conducting design workshops or discussions with community groups and leaders before any rollout.<br><br>Use this insight to select the right modality and workflow, and to design a community engagement and sensitisation strategy - including discussion, posters, consent workflow, helpdesks, and feedback channel - appropriate to the context.<br><br>Where a population has had significant negative experience, consider alternatives - or heavily 'front-loading' participatory design and community ownership of solutions. |

| | | |
|---|---|---|
| **Culture of liberties** | **Acceptance / False Acceptance** - where a group has little history of 'civil liberties'-based treatment of rights and freedoms, approaches built around individual consent and agency / explanation may be overwhelming or ineffective - leading to information overload or 'compliance-oriented' consent processes which are performative and meaningless. | Carefully consider the history in this population and whether there are alternative approaches - such as a non-consent lawful basis and stronger community engagement - which find the right balance of agency for the group.<br><br>Consider how to meaningfully offer Rights such as Access to data, De-Consent, or complaint processes with populations for whom these may not be familiar safeguards.<br><br>Where this is challenging, consider investing heavily in community understanding and capacity building with the target community alongside participatory design to enable them to revisit and feed into the solution over time as their understanding develops. |
| **Language & Digital Literacy** | **Transparency** - failing to consider the languages spoken by the population, the level of literacy, and the understanding of digital tools and how they are used - in particular where part of a complex digital ecosystem involving government and partners - may make consent meaningless or ineffective. | Plan and iterate an approach to transparency which is based on an understanding of the target group and their needs.<br><br>When planning resourcing for the project, ensure that the language and communication skills needed (for translation within the tech, rollout, and support at field level) meet the needs of the population.<br><br>Where this is challenging, consider investing heavily in community understanding and capacity building with the target community alongside participatory design to enable them to revisit and feed into the solution over time as their understanding develops. |
| **Location & Distribution** | **Inclusion** - where enrolment sites, helpdesks, or project staff are not distributed evenly across an intervention area - or may be peripatetic and change location or be less present once enrolment has taken place - an inability to access troubleshooting services may pose inclusion issues if subjects cannot quickly present with challenges such as false rejection or other access issues. | Carefully consider the need for helpdesk, enrolment stations, and distribution of staff - not only during the initial stages of a project but over its lifespan. |
| | **Acceptance & Agency** - Beyond inclusion issues, failing to make available trained staff who can explain, respond to concerns, or field requests for data, to opt-out, or spot problems early may result in acceptance issues or fundamental issues of agency (e.g. if Data Subject Rights such as Access or Deconsent cannot be exercised) long after the initial stages of a project. | Plan for the need of a population over the lifespan you are using the data, including:<br>- Providing ongoing and layered information about how data is used;<br>- Responding to concerns and complaints;<br>- Enabling the ability for subjects to access their data or opt-out, or exercise other Data Subject Rights. |

## Conflict

Areas which are subject to active geopolitical conflict will clearly be the spaces in which harms or data misuse may be most vividly imagined or understood. In 2022, the use of cyberconflict in warfare is ubiquitous and well-conflicted, with hundreds of discrete attacks reported over the opening months of the Invasion of Ukraine in 2022[18].

The reported breach both of USAID, the US Agency for International Development[19], and the International Committee of the Red Cross[20] clearly also present datapoints which suggest that Humanitarian Actors are targets in what has become a regrettably commonplace facet of the exercise of state power.

Responsibly understanding the risk of technology we deploy as humanitarian actors therefore requires accounting for this likelihood of parties to a conflict disrupting our systems or obtaining access to data as part of our deployment.

Beginning from this starting point of context assessment should support both the risk assessment process - giving rise to mitigations which may include heightened information security practice, greater caution in collection of identifiable data, or alternative programming - but also a decision to operate in the first place. While context-aware risk assessment may help manage this virtually omnipresent threat, 'building bigger walls' is often not a sustainable or intelligent approach.

In any conflict space, the key questions you will initially want to ask as part of your risk assessment are:

- Who are the actors party to a conflict?
- What motive might they have for disrupting systems or accessing data?
- How might the data we plan to collect affect the conflict or be of use to the actors?
- How might the conflict evolve in ways which may change these answers?
- How might we need to plan for its unplanned evolution?

In some instances, these answers might be sufficient to frame risk as either so significant or minimal that your risk assessment begins to take form from an early stage. If it does not - or the risk appears minimal - it may be useful to dig deeper - in particular using situational reasoning to draw comparisons between similar conflicts, or publicly available (or privately shared shared) data - where possible - about the behaviour and capabilities of parties to a conflict:

- What capabilities do the parties to a conflict have? What level of sophistication might their various organs have, for instance to compromise systems, disrupt or access critical infrastructure, cellphones, or deploy sophisticated information gathering tools?

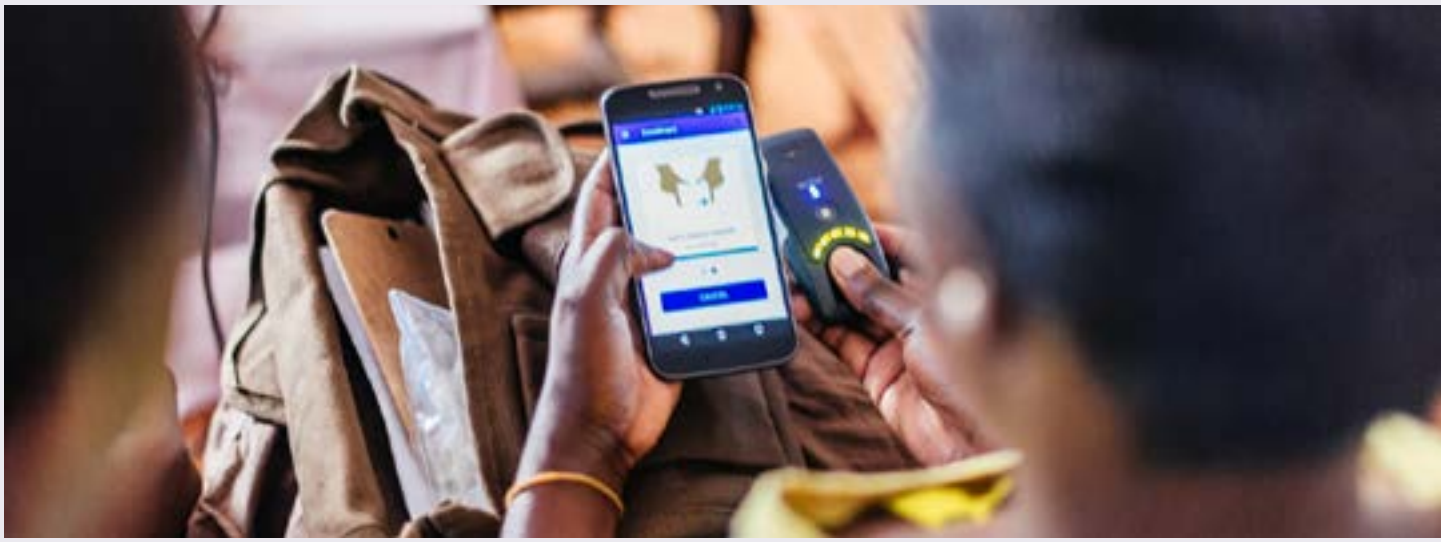
- What track record do they - or groups they align with or are sponsored by - have of introducing cyberattacks into conflict space?

- Are there other supporting state actors, allies, or miscellaneous groups such as criminal actors or 'hacktivist' groups who have similar track records of intervening?

18 Cyberpeace Institute (2022) - Conflict Tracker - Accessed at https://cyberconflicts.cyberpeaceinstitute.org/threats/timeline

19 Al Jazeera (2021) - Russian hack targeted USAID - Accessed at https://www.aljazeera.com/news/2021/5/28/russian-hack-targeted-usaid-human-rights-organisations

20 ICRC (2022) - Cyber Attack on ICRC - What we Know - Accessed at https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know



- Are there other regional conflicts or similar crisis points which we can learn from which have publicly available data about attacks?

- Are there industry, peer, donor, or institutional entities who collate 'threat data' we can access which might inform our approach (e.g. the government where our entity is domiciled)?

- How might the data we plan to collect affect the conflict or be of use to the actors?

Where this information is not readily forthcoming, discussion with peer groups, government, Information Sharing networks such as consortia, forums, ISACs, or peer networks may be worth leveraging to obtain or deepen understanding.

## Digital Ecosystem

It is often tempting - and easy, given the way funding and project rollouts work - to think about one's work in a vacuum, considering only one's own deliverables, tools, datasets, and participants. But the risk to participants is rarely so tightly bound to a single intervention - and may be heightened (or lessened) by the surrounding ecosystem and actors.

Therefore, consider as part of your risk assessment asking questions about the broader ecosystem and how it might affect the data you collect. You may find that the pre-existence of other infrastructure allows your data to be correlated with other sources, reducing its anonymity or heightening its utility. It may make the likelihood of 'scope creep' higher. You may even find synergies or alignment which enhance the effectiveness of your intervention or allow you to plan better for future developments.

In particular in countries which are rapidly building out digital ID and other 'citizen service' infrastructure - such as civil registration, health, social security, and other infrastructure - government systems and policy may have a significant impact on your work. And increasingly there is tight integration with data held by private sector actors, from Financial Service Providers to cloud technology providers with humanitarian teams.

Consider asking:

- Which other actors are deploying tech4dev or other tools - including peers, but also non-traditional humanitarian actors?

- What other technology is deployed in the environment already - what digital infrastructure exists which is run by government, private sector, or other actors in the host country?

- Does our deployment conflict with or complement these tools - would combining the data in the various tools affect the risk of their deployment?

- Does the existence of these other systems make the likelihood of scope creep larger?

- Which government digital tools are in the environment - for instance is there a Digital ID system or other National Registration which might affect our deployment or impact the risk?

- Are there any relevant government strategies - for instance for digitisation, digital transformation, data, or legal framework changes?

- If we're piggybacking on infrastructure - for instance the government or ATMs - does this introduce equity challenges based on location, positioning, registration, or known issues of inclusion?

- Where we're using shared infrastructure - for instance private sector cloud or FSP infrastructure - does this introduce additional use-cases, for instance if the data is used by the private sector actor to market or distribute other goods or services?

Aligning with the foundational assessment of needs and benefit which should underpin any project, the ecosystem should also inform a counterfactual - i.e. a 'negative' question - Does this intervention meet a genuine need, and is there other infrastructure which would achieve the need better or more effectively? As government identity systems and response environments become more complex, the most valuable thing an implementor can sometimes do is not to add another system to the mix.

## Partnership

A theme throughout this section of the handbook is the externalities ***outside*** our own work which impact outcomes - from geopolitics to worn hands from manual work. But one of the single largest sources of externalities of error and omission come from partner relationships.
The typical single INGO humanitarian intervention in 2021 may involve several dozen hardware, software and cloud platforms, including specialised data collection tools[21], mobile devices, Business Intelligence Tools, Laptop or Mobile devices, and cloud backends. Even a single-agency intervention may use dozens of cloud-hosted or separately-supplied software stacks - each supported by a different cloud or technology vendor.

And humanitarian interventions are rarely single-agency. Topologies vary, and range from simple partnerships or hierarchical sub-granting models to more modular collaborations[22]. These may have not only complex dataflows but also complex Controller identities and accountability models.

Increasingly, deep work is being done on responsibilities and safety - implementors are well-advised to engage with and understand this work, in particular as biometrics become a more

21 While outdated, the nomad project records 50 from 2016 - https://humanitarian-nomad.org/online-selection-tool
22 CaLP (2020) - CTP Operational Models Analytical Framework

ubiquitous part of the humanitarian response environment[23].

It is rarely the case that this chain is well-mapped out, and particularly at a program level typical that *"Technology and data processing [having] uses and consequences that at present are poorly understood by many humanitarian practitioners, project managers and policy advisers"*[24].

Any humanitarian will be familiar with the idea of 'partnership assessments', of which there are dozens of examples with various degrees of diligence and effectiveness[25]. But it is unusual for partnership assessments to dig deep into digital or data capacity and capability. At a project level, it is rarely the case that the nuance and complexity of data flow and responsibility is truly explored as part of organisations' work together.

When the responsibilities and remits held by different partners are not explored - and there is no significant conversation about how risk is managed - then it may not matter how effectively one organisation manages data or assesses risk. In the best case, the effective level of 'responsibility' across the entities involved may fall to that of the weakest actor - which data suggests may in some instances be a very low bar[26].

**Warning** - Without meaningful bilateral assessment - and transparency - agencies may not know if they are safe partners for each other. And without mapping out the collective and several responsibilities they hold, it will not be clear to anyone how safety will be achieved.

In the worst case, misalignment of objectives and approaches may actively damage partnerships, and a failure to agree on responsibilities can result in harmful lack of responsibility, scope creep, or a loss of trust by the affected population.

Therefore, factoring in partnership relationships ***must*** *be part of* the process of design and risk assessment we undertake to responsibly act.

There are likely, broadly, to be three categories of partner we need to consider:

1. **Simple subcontractors** - potentially including technology providers or subgrantees - with relatively straight forward divisions of responsibility - whom we largely 'instruct';
2. **Integrated partnerships** - such as coalition partners, subgrantees or prime contractors, with whom we work in a highly-integrated way, potentially under 'umbrella' branding or as part of monolithic projects or program structures, but who may have complementary but distinct objectives and activities;
3. **Complex and independent partners** - such as government institutions, large INGOs or International Organisations whose objectives are substantially distinct from our own, or private sector infrastructure providers whose tools we leverage.

These are to some extent overlapping categories - but reflect three different ways partnerships may be managed.

23 IASC (2021) - IASC Operational Guidance on Data Responsibility in Humanitarian Action

24 Goodman, R et al (2020) - Review and Analysis of Identification and registration systems in recurrent and protracted crises

25 ICVA - Partner Capacity Assessments of Humanitarian NGOs - Fit for purpose? https://www.alnap.org/system/files/content/resource/files/main/150610-partner-capacity-assessment-0.pdf

26 Goodman, R et al (2020)

*Simple*

Where a partner is largely 'instructed', managing the partnership risk is likely to be a simple case of first ensuring that the partner is a responsible and competent one (a 'due diligence') problem, and subsequently ensuring that the instructions provided are the right ones.

These partnerships most closely model the "Controller / Processor" topology envisaged by the GDPR as in effect the most common form of data exchange - and it should not be surprising therefore that many tools useful for managing these relationships will exist within organisations' data protection compliance efforts - such as "Data Processing Agreement" contracts which articulate roles and responsibilities, or policies, certification standards, or pro forma sales material outlining "Technical and Organisational Measures" or organisations' approach to Cyber and Information Security.

These tools and traditional supplier management tools are likely to be broadly effective ones for partners like this - designed as they are in effect to quantify and qualify understood and subcontracted responsibilities.

They will include including due diligence steps such as information security assessment of the partner's capabilities and policies (using an international framework such a ISO27001, Government standard such as NIST CMMC2, or some other framework - or even 'certifications' the partner provides) and other risk assessment and ethical procurement tools.

Instructions to the partner - likely issued and documented through commercial paperwork and transactions and/or the lens of a GDPR-compliant Data Processing Agreement - may happen almost automatically in maturer organisations, or where less mature be a simple matter of creative legal and technical problem solving using these relatively standard tools. In organizations which do not have prior tools for this, these - or other GDPR-inspired 'data sharing agreements' - can be good prototypes.

In some partnerships, other tools may be useful too - including due diligence on specific policies, technical audits, or "penetration testing" - empirical assessment of system security. Where the partner is a technology partner, this practical evidence of resilience and a program designed to engineer-in security-by-design should strongly be considered as a mandatory component of due diligence - a technology partner should be able to provide policies evidencing systematic application of an Information Security and Application Security lifecycle and practical evidence in the form of audits and penetration testing. Precisely what is 'right' for a given situation will be a question best balanced with specialist support from an information security specialist or team.

There are a few circumstances where even where the tools are right, they can be hard to apply:

Where a 'simple' partnership is **with a larger organisation** such as a cloud provider, maturity may be a double edged sword - DPA and Certifications may be readily-forthcoming but other questions difficult to answer.

And **where these partners are overseas** - in particular, where they are in countries with legal frameworks that offer weaker levels of protection for data when it is exported - it may be necessary to consider how this can be risk assessed via a tool such as a 'Transfer Impact Assessment' - a task best left to specialists and which may significantly increase program or partnership cost complexity.

Meanwhile, **with less mature suppliers or subcontractors**, it may be necessary to budget in time to 'coach' through these steps or 'lift the lid' - a less mature partner or provider may lack Information Security Policies or their implementation may be less mature - similarly increasingly the level of complexity when working with these partners.

### *Integrated*

Where partners have relationships which are not predominantly commercial or about service provision, the approach may need to be less simple. In particular, where organisations are peers who have subtly different programming - one might be carrying out food distribution whilst another might be working with subjects to protect them or build skills - data may be shared or integrated but organisations may have different donors or objectives. Or two organisations may be doing overlapping work on the same thematic and sharing data to ensure coverage, de-duplicate, or enable referral.

In these instances, whilst it may remain necessary to undertake bilateral review or alignment on policies, or undertake reviews of each others' information security practice - i.e. the 'Simple' tools - these steps by themselves may not address some harms. For instance, they will not ensure that in making complementary uses of data there is no scope creep, that pathways are maintained for hearing feedback, or ensuring the distinction between distinct 'Purposes' remains clear.

And in these circumstances, "I tell you, and you follow the contract" is unlikely to be the right model - and therefore so too are "Data Processing Agreements" with the Controller - Processor mindset. In Data Protection law, this type of partnership often has a different legal arrangement - sometimes referred to as "Controllers in Common", or sometimes a mix. There are various ways the law treats these arrangements - which option will be a matter of specialist advice tailored to the context.

What is most important is that a more complex partnership proceeds from the basis of an **understanding of the responsibilities held by the various parties** and where boundaries of separation - potentially ones aligned with the legal concept of the 'Controller' lie.

A set of responsibilities which can be used to map out some key responsibilities - based on good practice in data management and data protection practice - is given in this appendix.

### *Independent*

Not all partnerships will fit one of these models. Government and International Actors may work in complementary but highly separate ways - or require boundaries which preserve Immunities and Privileges or respect separate Purposes. Other partnerships between private sector and aid actors may share some common goals, but be built on fundamentally different business models and dataflows.

In these instances, partnerships may feel 'external', and data may be shared over relatively external boundaries which delineate responsibilities or accountabilities.

In these instances, partners are less likely to map out each others' responsibilities, and may prefer instead to undertake high-level due diligence of each others practice - or use tools such as Memoranda of Understanding (MoU) to align on working principles and practice & highly-

independent responsibilities - and subsequently work relatively autonomously within those capabilities.

In these instances, consider which ethical principles may need to be incorporated into an MoU or alignment; whether the distinction will be clear to Subjects and communicable when working with them; and what ethical issues - in particular deriving from scope creep or separate purposes - may be posed by the separate working.

There are no one-size-fits-all tools for partnerships such as this; but a crucial success factor is likely to be that **there is a clear separation of accountabilities and responsibilities**, that **it will be clear or communicable to Subjects**, that **both parties are aligned on common areas of ethical and risk practice**, and that where applicable **the right ethics/right due diligence is done** - for instance, understanding business model, future practice, and independent objectives well enough to understand what implications they may have for trust, harms, or reputation.

### *Conclusion / Resources*

Across all three sets of partnerships, the table in Appendix - Due Diligence and Safety Tools presents some of the available tools and mechanisms for producing mutual understanding, undertaking mutual due diligence, asking and answering questions about safety in the context of partner relationships which practitioners may find useful.

And - in particular for integrated partnership - Appendix - Skills & Responsabilities - outlines some of the key skills and responsibilities which partners may need to align, agree, and plan around between themselves.

## Consultation and Civil Society

Throughout this section of the guide, we have touched on consultation and inclusion as part of the design process in order to both answer questions we have identified and prompt those we might not have asked.

Consulting the affected group and iterating design of programming with them is the single most powerful way not only to answer 'known unknowns', but also prompt 'unknown unknowns' - as well as craft mitigations which may not immediately have been apparent when inevitably some of the 'unknowns' are hidden risks.

But beyond inquiry, the act of consultation itself is also an important act of respect which if done meaningfully will increase acceptance, and in some programs may be a bridge to meaningful ownership and transfer - of understanding, technology, and programing itself - to the population.

Strongly consider doing this in three stages:

1. Carrying out meaningful consultation as part of inquiry and design - potentially via a human-centered design approach, an integrated MEAL plan, or other activity which undertakes pilot work, hears the voices and feedback of subjects of the collection and data usage activity, and iterates program design;

2. Engaging the affected community more broadly - to inform and consult regarding how data is used as part of broader rollout - potentially also as part of integrated MEAL activity, but with a broader emphasis on communication and accountability, incorporating lessons from earlier pilot work

and focusing on aspects of collection or usage which may require deeper embedding (such as concepts, partner relationships or risks which are more challenging), and providing an ongoing channel to incorporate feedback;

3. Consultation of other civil society groups - in particular where an intervention is innovative, large in scale, or could be contentious. Which civil society groups are right will vary from context to context - but consider national, regional, or international:

   **a.** Human Rights or Digital Rights actors such as data or digital-focused NGOs;

   **b.** Groups working on behalf of marginalised groups and communities;

   **c.** Other lobbying or consumer organisations who are working to represent citizenry, or exercise statutory consumer powers.

Failing to make space for hearing and incorporating feedback can render an otherwise-effective intervention an expensive waste of money through low social and community acceptance. Meaningfully building in time and space for doing this from the beginning can not only ensure that expected outcomes and benefits are felt, but also represent a significant impact stream itself - strengthening and contributing to healthy, well-governed communities and spaces able to understand and respond to the way data is used well beyond the data your agency will collect.

## Context - Conclusion

Of course, the best questions often yield answers which are, themselves, questions - or at least hypotheses with more or less rigidly defined areas of doubt and uncertainty. The themes, prompts and risk assessment questions are therefore not intended as an exhaustive list of areas of doubt which if illuminated will result in an absolute moral understanding, but rather as a starting point - based on the themes and real-world harms which

have most commonly arisen hitherto.

In this fast moving area - where the ambiguity of attribution and nebulousness of actors' capability are themselves strategic assets - it can in fact be almost impossible to obtain clear answers with absolute diagnostic clarity. New forms of inequity and deeper understanding of the social and economic causes of disadvantage are continually being better understood.

The right level of certainty therefore will be context- specific, based on up-to-date learning, and should be linked to the harms we are attempting to avoid and the data and systems we are working with - as well as rooted in consultation and agency of the affected groups of humans.

Earlier in this guide we introduced the concept of threat modeling. When thinking about deliberate harms exercised by actors who compromise systems or may seek to misuse data, the form of 'archetyping' outlined above - i.e. loosely defining *who* may seek to disrupt our work, and establishing a 'good enough' sense of what they may be capable of given the data available to us as part of a risk assessment process - can be an excellent way to supplement or establish a threat model that allows us to make operational or programmatic decisions.

Consider your understanding here good enough if the level of effort exercised in asking and answering questions is proportionate to the problem, if the population has been meaningfully involved in the process of inquiry, and your understanding of the context is linked to the need/ benefit to the population.

In particular in your governed decision to mitigate risk and move forward that one of the following three conditions is true:

1. The **risk to your population and of your data is very low,** and you **conclude that you may not meaningfully be a target**, if the **benefit to the population clearly outweighs any risks** and on the basis of these factors and the safeguards you have in place, **if targeted little harm could come about**;

2. The **risk to your population exists**, and you **know enough about the adversaries** in your threat environment to form a threat model which feeds into your risk assessment and meaningfully enables you **to construct mitigations**, plan deployment, and implement controls which are **proportionate to the threats you see** - especially if triangulated with data from your peers or other third party groups - and in particular if **consultation with your population supports a conclusion that the residual risk is additionally outweighed by the benefits to the population**;

3. The **risk to your population is significant**, and you conclude either on the basis of what you can know about the adversaries in your threat environment - or the inherent unknowability of their capabilities - that **it would not be possible for you to manage risks OR undertake a meaningful Informed Consent process** with an At-Risk population - yielding a decision not to deploy, or do find an alternative.

# Safe Design & Deployment

So far, this guide has largely considered factors which may form part of the 'pre-deployment' planning, or which relate largely to people and context rather than technology.

But there are a number of factors - some unique to biometric technology - which should be considered when procuring a system for use or deploying it practically.

## Safety Considerations when Deploying

Some of these relate to the 'safety' of the technology itself - that is, that the technology in use allows us to meet requirements we have regarding Confidentiality, Integrity, and Availability, in line with general good practice, but the understanding which we have regarding the threat actors facing us, and our context.

### Data is Data is Data

Some biometric systems - particularly those which work online, using an active internet connection - may store data largely in one, 'master' database in a server or cloud system. Reducing the number of places where biometric data is stored can be beneficial for safety as it may reduce the number of places where protective controls need to be enforced to protect the data - defending one asset rather than many.

Where storing biometric data in centralised databases, it is typically regarded as good practice to store biometric data separately from other (demographic or programmatic) data - a practice sometimes referred to as **siloing**. Storing biometric data separately - in particular in a limited number of systems which are able to have more robust and restrictive controls applied, such as a limited pool of administrative users, separate authorization and authentication processes, and limited internal and external interfaces - is likely to make these systems harder to breach, and therefore increase the difficulty of an attacker gaining access to the biometric data.

However, there will be circumstances in which storing data in one location is impossible or undesirable. For instance:

- A solution that works offline will require data is cached or stored in some quantity on a mobile or field device;
- Where solutions are complex they may integrate many systems together, or integrate with partners or third parties which render 'one database' impossible;
- Some deployments may consider on the basis of policy or risk assessment that one data repository is undesirable, or adopt a different privacy/protective approach -

storing data only on local factors held by the user, in a distributed storage platform such as a blockchain, or use another privacy-preserving technology which functions differently to a traditional storage paradigm.

## Integrations

Where systems are **integrated,** careful consideration should be given to the nature of the integration, as well as what data interchange is necessary to enable the integration.

It is often not necessary to synchronise full databases - including biometric templates or material - with other systems in order to enable an integration for de-duplication, to refer participants, or for other purposes.

Alternatives include pseudonymous approaches - which make subjects more difficult to identify by partially de-identifying data, including those using a tokenisation-based approach - in which a random or substitute value is stored in a 'master' database in lieu of the biometric data itself.

The advantage of these approaches is that even if an integration is compromised, the harm to subjects may not be automatic, and mitigating steps may be available which are unavailable if 'all data' is synced.

Reduce integrations and treat them thoughtfully wherever possible - consider them as part of the overall security architecture when undertaking threat modeling, risk assessments, or assurance activities such as security testing.

Where systems are heavily integrated, ensure that risk and impact assessments are clear in scope and extent - clearly ending at integration points and shaping partnering discussions regarding responsibility which align with what subjects are told, ***or*** taking these integrations into account and treating their full extent where appropriate.

## Local and Distributed Storage

Alternatively, some solutions will store biometric material on a smartcard, in a digital wallet, or in some distributed location which moves away from a traditional 'legal entity as custodian of data' model - sometimes touting benefits to the subject such as direct individual control, or reduced reliance on gatekeeping, custodial institutions.

These solutions may offer benefits such as enhanced trust and control, or reduced (or largely eliminated) attack surface, by eliminating centrally held databases which are immediately attackable by an adversary.

However, there are trade-offs with these designs. Functionally, distributed or locally-held data may reduce the ability to benefit from tools which can only be implemented centrally - such as intrusion detection, functional tools like de-duplication, or certain forms of encryption. It may also be difficult to reissue cards where lost or stolen - without also storing data centrally.

Further, with a disempowered or unaware population, the benefits of 'individual control' may be reduced where a population cannot refuse to hand smartcards containing template material to a malicious actor.

Decentralised storage will be the right solution for some use-cases and the wrong solution for some. Where considering it, care should be given to understanding the functional limitations and implications in specific contexts - linking the analysis carefully to an understanding of threat actors and risk factors.

And lastly, in the design of the solution, care should be taken to choose the right encryption technology or privacy-preserving techniques used to store the data on a locally-held or distributed factor. There are myriad options available, from traditional encryption which 'locks' data on a card using a key - for instance a PIN number or passcode - to approaches which leverage high-density QR or graphical storage and hashing or Template Protection techniques and tokenisation which offer more sophisticated protection, locking the cryptography to the user's biometric factor itself or reducing the amount of data available for theft on the factor.

Understanding and assessing these approaches is arguably a career specialism in itself - implementors choosing or relying on one of them should be careful to ensure they have the capability to choose carefully and integrate the choice into their analysis and operational practice - understanding and aligning the security controls offered by the technology to their threat model and what is communicated to the subject.

### Traditional Encryption

Traditional 'encryption' is often reduced when considering systems security to approaches which protect data 'at rest' - that is to say, encrypting storage devices, computing or mobile devices, or the data held on them when it is stored and not in use - and 'in transit' - that is to say, encrypting data as it is moved from device to device or data silo to data silo.

Generally, when we refer to one of these types of encryption we will be referring to an approach which has in effect encapsulated the data which we wish to share - a full biometric template, database, or dataset - inside a protected wrapper which can only be unpeeled given access to a 'secret' referred to as a key. The raw data - usually referred to as plaintext - is turned into encrypted data which is usually referred to as 'ciphertext' using an encryption algorithm which is essentially complex mathematics.

Cryptography is a complex field best left to specialists, but a generalist should understand that traditional cryptography relies on keeping key material safe in order to sustain the protection offered by encryption. This means in practice that in the cloud - or on a server, mobile device - which must *work with* data the key must also be present to unlock the data, and data will necessarily be 'exposed' - available in plaintext, or unencrypted - while being worked with, either in computer memory or regularly.

This necessarily limits the effectiveness of encryption to mitigate all forms of misuse in two key ways:

Firstly, the strength of encryption as a protective safeguard is only as good as the 'key handling'. Where keys are stored alongside data, linked to a PIN code or stored in protective storage on a device, the strength of other controls, the PIN code, or the protective storage will necessarily be the limiting factor.

Secondly, where data is regularly worked with data will inevitably be exposed. Encryption cannot by necessity - and does not claim to - offer 100% protection to theft on 'in-use' devices. Cloud assets or laptops which are breached, mobile phones which are remotely compromised using sophisticated malware may contain *encrypted* data when powered down or unattended, but are still vulnerable to various forms of attack.
It is sufficient for a generalist to understand that this is complex, and that "it is encrypted" is rarely

an absolute answer to a question about the impact of a breach, safety of a product or solution.

But where deploying or procuring a solution, care should be taken to understand - fully - how any encryption techniques employed work, what their limitations are, and where they fit into a broader threat model. What do you truly care about, and does your cryptography care too?

## Next Generation Encryption

In recent years, a variety of novel and complex techniques have begun to enter the marketplace and thought ecosystem - including techniques such as Quantum and Homomorphic Encryption.

Many of these are best left to specialists and are years away from standardisation and commercial availability - but in the field of biometrics in particular, innovators should be in particular aware of the claims and possibilities of **Homomorphic Encryption**, a technique which breaks the model presented in the previous section and *allows encrypted data to be worked with while not losing its protection or requiring such careful key management*.

A technique using **Fully Homomorphic Encryption** (or **FHE**) might for instance allow two partners to share an encrypted database between them which allows either partner to query the database for a match - establishing, for instance, that Subject S received services from one or both organizations, or is on a list of at-risk individuals - without *seeing* the database itself, rendering it significantly less vulnerable (and therefore the full set of Subjects significantly less at risk) if the database is stolen, irrespective of whether or not it may be in use at the time.
Other possibilities include de-duplication without viewing data, or querying for subsets of participants (e.g. extracting an encrypted set of "Subjects who received food assistance last year" without seeing the list) - again while retaining the 'protective wrapper' offered by encryption.

FHE has some limitations. Many current solutions are computationally expensive - limiting their deployability in low-resource settings. And the technology is broadly early in its innovation cycle - heavily limiting the number of 'field-ready' solutions, as well as expertise available to deploy it.

And at a national and cultural level, little regulation or standardisation yet exists - or social understanding and acceptance of the technology.

There is cause therefore for both caution and optimism - that FHE in particular may present significant opportunity to reduce risk, but caution would be well-advised for all but the most mature and low-risk of implementors at present.

If these technologies do appear to offer solutions for your use-case, proceed carefully - link them rigorously to your threat and risk model, plan-in realistic timeframes, ensure you have the right skills and competencies to understand what you're working with, and bake-in considerable resourcing to engage with the communities you're working with and build their confidence, knowledge, and trust.

## Software is Software is Software

Whatever specific protective technology is incorporated into software which may reduce the impact if data is stolen or protect it from theft, software itself fails.

Security engineering remains a relatively young discipline; building safe, resilient software is

complex, and with millions of moving parts and dozens of technologies and components in many software products, the number of potential 'failure modes' which need to be avoided when writing code, assembling, and implementing can be enormous.

In highly-regulated or high-security environments, large teams of engineers, senior security specialists, architects, and others bring (expensive) structure and discipline to bear in meeting this complex set of challenges. But many technology organisations are still evolving their approaches - producing in part the continuous news cycle we witness of vendors and corporations being 'breached' when they don't get it right.

Unfortunately, as an implementor the difference between a vendor or supplier building highly robust and resilient software and one whose tools require the 'buyer beware' can be difficult to distinguish between in this yet-unsolved problem.

Earlier in this guidance we touched on the subject of partner assurance - that is, coming to an understanding that a partner has the right tools, policies, and controls - often as part of a 'due diligence' process during procurement.

When developing or procuring software, it is typical to undertaking various forms of 'assurance activity' to ensure the quality of the final solution or integrating various technical or procedural steps into a development lifecycle to promote high-quality software.

At its simplest, 'assurance' often looks like a 'one-stop' assessment activity such as a "penetration test" or security assessment designed to assay the quality of something - a little like a building survey or inspection.

However, these 'point in time' approaches - while necessary during commercial transactions - are relatively poor substitutes for 'systemic' approaches which integrate policies, training, automated technical solutions, and process controls, and attempt to ensure that a vendor is 'resilient' and not 'evolving'.

When designing software, there are various frameworks such as the Building Software Security In Maturity Model (BSSIM) which propose and categorise some of these activities - as well as bodies curating guidance and good practice in the area of application security such as OWASP - which suggest what some of these lifecycle elements and steps are.

Where procuring or assessing a biometric solution for suitability in any development or humanitarian application - even relatively low risk - the implementor would remain well-advised to ask for 'point in time' assurance via a well-scoped security test, but to regard this as 'necessary' and not 'sufficient', incorporating into their assurance and assessment process also:

1. A requirement or assessment for 'by-design' treatment of application security which is built on foundational disciplines of risk assessment and threat modeling which base technical design decisions on anticipatory practice;
2. An assessment of 'the human factor' - training and competence of staff, process and procedure;
3. Consideration where applicable of technical controls such as automated checks during the development lifecycle.

Where implementors do not have the knowledge in-house to ask for or understand the quality of these practices amongst their subcontractors or

suppliers, they should consider carefully whether they are ready to procure this type of software or if they need to budget for more internal resourcing or specialist advice to support them along the journey.

## Privacy Considerations when Deploying

The previous section dealt in depth with some aspects of systems security - including techniques and approaches for protecting data itself.

Privacy and ethical considerations rely on robust security practice; it is challenging to make good decisions about others' data when you lose control of the data.

But more broadly, once this (low) bar is cleared, privacy and ethical practice being about the 'how' they are (generally accurately) viewed more as disciplines more of people, practice, and governance than specific technical controls.

That said, there are some technologies and techniques which are distinct from foundational security controls and can genuinely add to the privacy-by-design posture of biometric systems.

The boundary between 'security-preserving' and 'privacy-preserving' can often be blurry - but in this section we deal with both sets of concerns - that is to say:

1. *Technical considerations which relate more to privacy* than security, and
2. *Other facets of responsible deployment* once the technology is procured, implemented, and ready which have not been covered explicitly elsewhere.

### Privacy Tech

Earlier in this guidance we have already referred to concepts such as **siloing** and **pseudonymisation**. Pseudonymisation is the practice of modifying data to link it less closely with specific, identifiable humans. A pseudonymised record might look like a patient record with only an ID number and medical notes, or research interviews with aliases rather than names.

Pseudonymised data may be re-identified by users - or a malicious actor - for instance by cross-referencing the ID numbers with another data source, or using the data itself to reidentify people.

The border between pseudonymous data and anonymous data can be a grey one; but by increasing the difficulty of reidentification, pseudonymising data - combined with separate storage - significantly increase the protection offered to individuals by increasing the difficulty of misuse.

While the examples given so far are largely procedural, some tools offer automated solutions for pseudonymisation, such as **tokenisation** - literally replacing data itself with a **token** which is less harmful than the data. These approaches have become commonplace in some sectors, such as the Payment Card sector, where replacing card numbers with a 'derisked' data string can reduce the impact when non-payment data is stolen.

While these techniques do exist in the biometric technology space, they are not yet ubiquitous, and should be carefully examined where available to understand the level of protection offered.

Amongst the most mature techniques include **Biometric Template Protection (BTP)** schemes - defined in ISO 24745, and implemented in

some reference and commercial implementation schemes.

Template Protection schemes may robustly reduce risk for some implementations, but will need to be carefully considered in line with broader requirements as well as the risk of the specific context, aligning the protections offered by properties such as **irreversibility**, **cancellability**, and **unlinkability** with the context and the threat model it presents.

A highly specialist area, implementors should be aware - as with all emerging technology - that the claims made by research or marketing material should be rigorously verified, and as with FHE organisations who do not have in-house capability or deep partnerships with specialists should not be relying too heavily on claims made by this technology without undertaking this rigorous verification.

It is sufficient for generalists to recognise, however, that these technologies exist - and are likely to be necessary to offset the seeming inevitability of the failure of protective security controls - and mitigate harms to individuals - particularly in use-cases with threat models involving determined attackers and over longer timeframes.

### Potential for Re-Use

Of critical concern when understanding the risk associated with a deployment which already has a specific **purpose** is - can that purpose be adhered to?

In particular, can the principle of **'purpose limitation'** - keeping, for instance, data collected for food security programming to be used for *only* that work and no more - be adhered to in a particular context.

An informed practitioner may intuit that some privacy and security safeguards - such as distributed or encrypted storage - may be useful to prevent egregiously 'excessive' over-purposed uses of data. Data inaccessible to field staff via access control or encryption may, for instance, prevent field or operational staff from recycling or sharing data thoughtlessly and in an ungoverned manner.

BTP schemes may negate some use-cases entirely - for instance, preventing linkage across systems.

Yet very few technical controls do not have an exception handling process, master key, or workaround. Even BTP and exotic techniques such as FHE have shortcomings, or may yet remain to be implemented.

The key foundational consideration for many projects may therefore be:

1. Robust governance internally and with partners - ensuring that purposes are clearly documented, known, and that internal controls exist which require robust signoff in the event of changes or 'edge-cases';

2. Risk assessment during implementation which anticipates circumstances in which there may be external or internal pressure to repurpose data which can:

    a. Be planned into the lifecycle of the data OR;
    b. Trigger a decision not to deploy in circumstances where purpose limitation cannot be reasonably expected to be upheld AND;
    c. Where possible evaluate and understand the use of technical solutions such as BTP, Cryptography, or other PPTs and their ability to negate anticipated misuse.

Much like more mundane aspects of data responsibility such as retention, accuracy, and broader hygiene, there is almost no escaping the requirement for operational discipline in upholding this principle once data has been collected, but the ability to exercise this discipline should nonetheless be assessed-for while deploying.

### Other Data Protection Considerations

Practitioners own data protection guidance should also provide robust inherited guidance on facets of data handling which are not specific to biometrics - including but not limited to Retention, Disposal, and Contractual Governance.

These "data lifecycle" practices, which are well-treated in other guidance[27], while not treated in depth in this guidance due to the relative robustness of existing foundational data protection guidance, nevertheless remain critical during operational deployment both for biometric and other data, and must inevitably form part of implementors' Impact Assessment of their work.

## Consent & Transparency

Research and inquiry into individual experience of digital identity solutions points frequently to individual distress, misunderstanding, and disempowerment as an accompanying ill where biometric and identity tools are rolled-out thoughtlessly[28] - suggesting that communities are frequently afraid, distressed, disengaged, and disrespected when we are not considerate and compassionate in working with them.

These serious challenges cannot be addressed purely in how we approach the act of data collection itself. Many have deeper roots in communities' relationship with power and assistance, as well as the broader factors shaping program agendas, issues of displacement, conflict, and resettlement.

But whatever these broader factors, the moment data is collected is the 'touchpoint' most participants will identify most closely with the activity - as well as a critical moment at which safeguards and respect may be embedded - or forgotten about.

No guidance on responsibility in data collection and use would be complete without treating this moment - where we embed principles of **transparency**, of **consultation**, of **choice**, and potentially of **informed consent** into our project; while not sufficient to resolve all ills in a challenging, risky, or poorly planned project, these cannot be understated as key moments in the privacy and broader responsibility position of a project or intervention.

### Transparency

Perhaps the least controversial aspect of this transactional moment is the information communicated to the subject regarding data which is collected from them, obtained from other sources, which may be produced, and which will be used by the responsible entity (and potentially its partners) to carry out some activity.

This **transparency information**, sometimes delivered via a **fair processing notice** or **privacy notice** is a requirement of most data protection

27 ICRC (2020) Handbook on Data Protection in Humanitarian Action - Accessed at https://www.icrc.org/en/data-protection-humanitarian-action-handbook

28 Schoemaker, Emrys (2021) - Identity at the margins: data justice and refugee experiences with digital identity systems in Lebanon, Jordan, and Uganda

legislative frameworks, and will form the basis for any fair and equitable collection of data - the ***communication to the individual of what data will be used how, why, and for how long***.

There are a raft of legal requirements relating to transparency - in Article 13/14, the GDPR articulates a Minimum Viable Product which ranges from the identity of the organisation to its purposes, and the rights held by the individual. A full list of these factors - together with brief commentary on ***the key benefit to the subject*** - is given below:

| Information | Benefit/Meaning to the Subject | Complexities in humanitarian and development settings |
|---|---|---|
| **Identity and Contact Details of the Controller** | Knowing the identity of the accountable organisation(s) is a critical factor in ensuring that they remain accountable to individuals - and that individuals can where needed seek redress, follow up with concerns or queries, and exercise rights. | Where dataflows are complex, there may be many organisations involved; the nuances of responsibility and long-term ownership of data may make this time-consuming to resolve and understand.<br><br>Contact details may be challenging to provide where programming is time-bound, locations are remote, and individuals may not have access to phones or e-mail.<br><br>"Redress" or complaint may not be as meaningful to a disempowered community or in a context where there is not robust rule of law, high literacy, or a culture of civil liberties. |
| **Contact details of the DPO** | Having a specific individual to engage with in the event of complaints or concerns. | |
| **Purposes of the Processing** | The 'Purpose' is a critical factor in allowing individuals to understand intent, consequence, and potential risks. Communicating it in plain language is a critical factor in ensuring individuals understand the structures and factors they are interacting with and affected by. | The purpose may not be clearly defined - as a result of low data maturity, or programming which is simply open-ended.<br><br>There may be multiple complementary or competing purposes - especially in a complex response environment.<br><br>Failing to consider purposes up-front due to poor planning or maladministration may seriously impact implementors' ability to make use of data which would be beneficial to subjects. |
| **Legal Basis for the Processing** | The 'Lawful Basis' is a construct in European and other Law which represents a key legal test 'unlocking' the use of data. Exposing the choice of basis allows subjects to challenge, understand which rights they have, and ensures organizations are accountable. | In practice, for many subjects this may not be a meaningful concept or possible to explain effectively. Implementors may also be poor at selecting and analysing which basis to use - even where this is a legal requirement for them.<br><br>Nonetheless , whether or not it is meaningful to 100% of subjects implementors *must* consider how they can expose this meaningfully (alongside purpose and other contextual factors) to be meaningfully accountable, and these (sometimes esoteric) concepts should be carefully and sensitively explored - even if they will not be engaged with by many subjects - as part of the overall compact of 'fairness' with the population. |
| **Legitimate Interests (where relevant)** | Where the lawful basis is LI, the law requires the "interest" of the organization is disclosed to the subject, effectively preventing "Just Because" data collection where the 'because' is not disclosed - allowing both individual understanding and where appropriate challenge. | |

| | | |
|---|---|---|
| **Recipients of the data** | Much like the purpose, the law anticipates that subjects should understand to whom data will be shared - which may itself be a critical risk factor. | Like purpose, organizations with lower maturity may find this harder to analyse - and it may change throughout implementation.<br><br>For many humanitarian recipients this will be difficult to contextualise and explain, and organisations with lower maturity may similarly not have mapped this out - although immaturity will not protect users or enable compliance with (or allow a flexible aprpoach to) the law. |
| **Transfer to third countries** | Some countries have lower legal safeguards - and fewer opportunities to challenge the use of data. The law anticipates that subjects will want to know this in instances where it could expose them to harm. | |
| **Period of storage or criteria for determining it** | The time period across which data is used represents an important 'bounding' factor in understanding *when* subjects may experience consequences. | |
| **Existence of Data Subject Rights** | European Law anticipates that the Data Subject Rights - to access data, challenge its use, deconsent, restrict use of, and otherwise impact the handling of data by controllers - represents an important part of the overall fairness and equity.<br><br>There are some of these rights which will be very important to humanitarian subjects - such as the Right to be Informed. And some subjects may need or wish to access data or deconsent - in particular in the event of a critical incident. | Especially in the white heat of a response, it can be challenging to explain why these compliance-heavy obligations are more important than a distribution, or the amount of paper and process involved is genuinely meaningful. An uncompassionate deployment of european transparency notices which presents service recipients with boilerplate legalese informing them of some esoteric rights is, indeed, unlikely to provide meaningful privacy protection.<br><br>But some passive rights - such as the right to be informed - will be important from the first moment of contact. And the other rights will nevertheless remain important to subjects as data use develops, the white heat subsides, or concerns do arise. |
| **The right to withdraw consent (where relevant)** | Where consent is used as a basis for collection, the law requires that users be able to deconsent; and anticipates that users must be informed of this individual power. | |
| **The right to lodge a complaint with a regulator** | When data use is truly unfair or a breach has occurred, the law anticipates that regulators and legal recourse are the final options available to individuals. Some subjects will benefit from knowing that they can access a third party to express concerns - and this right will in some instances be critical to them. | |
| **Factors relating to legal or contractual requirements to provide data - and consequences of failing to comply** | Where data collection is compulsory for contractual or legal reasons, this anticipates subjects should understand the constraint and be able to consider the effects of noncompliance - for instance, where employment is contingent on providing data and could be withheld if they do not wish to provide it. | |
| **Existence of (and information about) Automated Decision-Making** | Where Machine Learning, simpler automated thresholds or triggers, or any other piece of automation may make a consequential decision about individuals or their access to services or goods, the law sets out to ensure they understand - and can seek a human review of this. As use of AI/ML solutions or remote programming other modalities involving automation become commonplace, this is likely to be vital too for service recipients. | Contextualising and compassionately communicating this information may be hard - especially where it is ubiquitous or could be hard to challenge or implement manual processes for. |

| | | |
|---|---|---|
| **Further information about any other Purposes for which data may be processed** | Where secondary uses of data are anticipated - for instance, a piece of government programming which leverages the same data but to implement immigration control or long-term social development - the law anticipates that individuals must understand - as these additional uses may not be 'homogenous' in their impact on the lives of individuals. Knowledge may enable individual decision-making, use of the DSRs, or expression of complaints or concerns. | Implementors may not always know at the outset - this is anticipated in the GDPR, which makes further provision for this - but in addition may be hard to communicate (or know) due to the complexities of the operating context or other circumstances specific to the individual. |

European Law - and broader good practice - is rigid in requiring that all of this information is available to subjects[29] and provided at time of collection (with some exceptions and consideration of indirectly-acquired data[30]) save in rare instances - such as where the subject may already know, or communicating it "proves to be impossible or would involve a disproportionate effort"[31].

Even where interventions do not need to meet the comprehensive requirements of the GDPR (or organisations have yet to achieve full compliance), these detailed requirements are thoughtful, reflecting a layered and interlocking approach to privacy where purpose, basis, and various technical requirements are integrated into a conversation with individuals.

The law - and broader good practice and regulatory guidance - also anticipate that while a 'compliance-oriented' privacy notice may provide all of this information in a policy document or long-form written form, provision of information should be contextual, may be layered, and should emphasise specific (and the most important) details.

The table above attempts to prompt consideration of which pieces of information may be most meaningful - or should be accompanied by further training or signing (individuals may need, for instance, to be coached through what 'deconsent' means - or on what 'automated decision-making' is).

Good practice - both Privacy and in broader Accountability - suggests that in addition to the 'what', we should consider as part of a 'good practice' approach:

1. How this information is delivered - i.e. not only whether it is delivered verbally, on paper, on screen, or via some other medium at the 'moment' of first engagement or collection - but also any supplementary explanation, graphics, or sensitisation;
2. When it is delivered - i.e. that it is delivered at moments that make sense for the individual and community, potentially via workshops, written material, follow-up sessions, and other consultation or sensitisation processes;
3. How it is contextualised - i.e. that risks, future use-cases, and benefits are clearly identified along with more mechanical aspects of data use and retention.

However these nuances are explored, and whatever minimum set of 'information' you consider necessary to your use-case, it is vital also that:

29 GDPR, Article 13, 14, Right to be Informed.
30 GDPR, Recital 61
31 GDPR, Recital 62

**A.** What you communicate and how you communicate it is rooted in your contextual assessment of the individual, the risks, and the broader context;

**B.** You build a meaningful evaluation process into the design of your 'transparency' process, seeking to understand whether individuals genuinely understand and whether your process has shortcomings.

## Choice + Fairness

Harder than what you communicate is what choice you can offer. Legal approaches to the protection of individuals often acknowledge that choice may not be possible - recommending it where feasible but acknowledging explicitly through structures such as the Lawful Basis[32] that there are circumstances in which legal requirements, compelling need, or even lifesaving care which preclude being able to offer a serious choice.

### *Lawful Basis*

In data protection law, the Lawful Basis is best understood as a sort of 'gateway' to fairness for a data-using activity. Each lawful basis in the GDPR represents a different 'locus of agency and fairness' or 'social utility test' - some acknowledging choice, others 'overriding need' or compulsion from law.

While each basis comes with subtle differences - some introduce specific rights (e.g. Consent comes with a corresponding de-consent right) and others must be explained in different ways - ***none*** exempts the responsible organisation from a majority of its other obligations - including risk assessment, transparency, or proportionality.

Amongst development and humanitarian interventions, the most typical 'chosen' basis is one of the following four:

- Consent (Article 6(1)a) - i.e. the user can freely choose;
- Legal Obligation (Article 6(1)c) - i.e. collection is required - perhaps to comply with financial regulation, principles of the common law, or charity/NGO regulation;
- Public Task (Article 6(1)e) - i.e. collection is required to carry out some task in the public interest such as a healthcare or social activity - or the organisation has some other statutory mandate for its work;
- Legitimate Interests (Article 6(1)f) - i.e. there is no 'other' lawful basis, and the organization "just needs it" for some overriding intent which isn't overridden by the interests of the individual subject(s).

Implementors experienced in data protection will know that the choice of basis is complex, there is hidden depth, and evaluation needs to be made on the basis of a specific program, the nuances of an organisation's domicile, and potentially given legal advice.

### Consent

Yet one of the lawful bases stands out from the others - the basis whose root is 'choice' rather than internal or external factors - the **Consent lawful basis**.

This basis anticipates that there may be circumstances in society where an individual can truly choose to have their information used - holding all of the power, based on an informed and exercised individual liberty.
The GDPR lays out a deep and detailed

32 GDPR, Article 6

understanding of how and when this can be undertaken. It is in particular feasible only where revocable, freely informed, and unconditional for service[33]; and further in the regulatory guidance as deeply rooted in an understanding of power - and unobtainable where the Controlling organisation wields power over the individual[34].

This suggests that in development or humanitarian contexts in which service recipients are frequently dependent on aid agencies Consent is unlikely ever - in data protection terms - to be defensible as a safeguard of individual rights with respect to data. Various organizations have already published guidance explicitly suggesting that for them, consent as a lawful basis - rather than a more general ethical practice - is not feasible for them, including in the context of humanitarian biometrics[3536].

These policy changes should be read alongside ethnographic and other research into the individual experience when data is collected - which rarely if ever paints a picture of an empowered, libertarian response environment where subjects are truly agents of their own destiny, bought into the process of data collection and able to make choices unencumbered by outside influence and based on a full, frank understanding of data and systems[373839].

Where perfect choice cannot be offered - this does not mean it should not be attempted, or the law be read to infer that organizations can 'collect away' leveraging other pathways without remaining accountable, transparent, or privacy-centric.

But these other approaches should be understood to shift the 'burden of agency' - away from individuals who are compelled to make an unmakeable choice - and onto institutions who choose to continue to collect data where individual liberty is reduced.

This *institutional obligation* also carries with it an undertaking to undertake deeper risk assessment, and hold greater accountability for programmatic and risk outcomes - burdens explicitly recognised in legal treatment of non-Consent lawful bases such as the 'Legitimate Interest Assessment' and which should also be reflected in Impact and Risk Assessment.

**Warning** - Blindly using any lawful basis - but in particular the Consent basis - independently from project planning, privacy and security safeguards, and in particular a theory for community and individual engagement, consultation, choice, and transparency - is likely to lead to intrusive, disrespectful use of data. Consider the choice of legal pathway thoughtfully and as a complement to other safeguards and practices.

## *Choice*

Yet whatever legal analysis organisations do, choice is clearly desirable - and clearly dependent on understanding.

We suggest therefore that the minimum standard for responsible biometric deployment in these contexts - whatever the legal analysis - should be that:

33 GDPR, Article 7
34 Guidelines 05/2020 on consent under Regulation 2016/679 , EDPB
35 Oxfam (2021) - Biometric and Foundational Identity Policy
36 ICRC (2019) - Policy on the Processing of Biometric Data
37 The Engine Room (2020) - Understanding the Lived Effects of Digital ID
38 Schoemaker, Emrys (2021) - Identity at the margins: data justice and refugee experiences with digital identity systems in Lebanon, Jordan, and Uganda
39 Weitzberg et al (2021) - Between Surveillance and Recognition: Rethinking Digital Identity in Aid

1. Individuals are **offered sufficient understanding to comprehend how data is intended to be used** - and how it may be used outside this intent (taking into account future programming and any risks);
2. Individuals are **offered where viable an alternative to data collection** to engage with program activity;
3. But that where this is truly impossible - and the 'choice' offered is disengagement with an activity or program, particularly if legal constraints make choice in data collection impossible - **the inability to offer choice is considered throughout program design and implementation**;
4. This should inevitably be layered, comprehended, and safeguarded through the use of non-Consent lawful bases where applicable.

In these cases - where organisations "just need to" collect data, or have no legal recourse to allow an 'opt-out' - for instance if data sharing with government is a conditional of operations, or other requirements such as Know Your Customer (KYC) require it - these 'constraints' and implications should be communicated with abundant clarity to the affected population - being tested, evaluated, and the approach iterated during piloting and rollout.

## Local Legal Requirements

Funders, Implementors, and Operating Contexts may all bring with them different compliance and legal requirements. It would not, in fact, be atypical in 2022 for a development intervention to carry three or more distinct data protection frameworks all of which require treatment - one following the money (and an underlying choice to intervene, perhaps carrying with it elements of a donor's strategy), one the home domicile of the implementor (and key design decisions - maybe strategic or more tactical - as well as registration and compliance strings), and one the country in which program work is taking place (and therefore the legitimate rule of law within a context whose government is ideally accountable to the subject themselves).

Across the Global South, governments are introducing and exploring data protection legislation - or updates to previous instruments, with 71% countries implementing some legislation, and a number of other countries in the process of drafting it[40].

While in some cases, these mirror or align with the European legislation which affects many development actors - such as the Kenyan Data Protection Act - in other cases Data Protection and Cybersecurity instruments can contain significant differences or even stem more from a Government's security agenda than the protection of its citizenry[41].

The homogeneity of the words 'European Regulation' disguise, too, differences amongst European governments in implementation of the GDPR, the complexity of countries who may choose to leave the European Umbrella - and of course, the number of US and non-US/EU-based development actors and funders who are variously regulated and unregulated.

Assessing 'the law' is therefore an almost unavoidable part of any responsible deployment. While this guide is not a substitute for in-depth

40 UNCTAD - Data Protection and Privacy Legislation Worldwide (https://unctad.org/page/data-protection-and-privacy-legislation-worldwide)

41 AccessNow (27/1/2022) - Analysis: the Myanmar junta's Cybersecurity Law would be a disaster for human rights (https://www.accessnow.org/analysis-myanmar-cybersecurity-law/)

legal guidance, the most significant constraints which legal frameworks bring are, in broad strokes:

1. **Explicit additional requirements around biometrics** - such as the 'Special Category' framework in European Law, or separate regulation of biometric collection such as the Aadhaar Act in India.

2. **'Binary' Treatment of Consent** - where legal frameworks do not share the GDPR's complex 'lawful basis' framework and there may be a hard requirement to 'obtain permission' or 'obtain consent' to data use and collection.

3. **Requirements to share or disclose data**, or a less explicit but similarly impactful **reduction in protection from requests or requirements** to share or disclose to government or other authorities - or other Safety or Cybersecurity requirements which oblige behaviours, logging, sharing, or other steps.

4. **Data Residency Requirements** which prevent export of data or impose complex constraints such as 'appropriate safeguards' where taking data across borders - and may pose implementation challenges, as well as putting data closer to legal orders or seizure within the operating context, or precluding the use of certain cloud tools.

Context assessment - and partner due diligence - should make sufficient time to understand these constraints both in terms of their compliance impact as well as their broader functional and privacy-preserving impact (positive or negative). Where assessing the implications of local regulation, care should also be given to consider:

- **Non-statutory policy or other informal practice** (particularly if working closely with government) - which can often impose requirements almost as stringent as statutory requirements;
- **Level of enforcement & understanding within civil society** - particularly if local law is relied upon as a privacy safeguard for Subjects, but may not be robustly enforced and understood;
- **Planned or future regulation.**

## Inclusion / Quality Considerations when deploying

Irrespective of planning, social contract with individuals and communities, risk assessment and benefit - if the technology does not work when finger meets sensor, or photos are captured by camera, it may yet not be fair or equitable.

In particular, with biometric technology - which we know relies on probabilities and thresholds - the externalities posed by 'real life' - from dust to digit selection - introduce complexities which if not accounted for may pose serious inclusion issues, excluding some participants or regions, or rendering patients enrolled by some staff more likely to benefit than others.

Thinking through the biometric capture process itself - both at initial enrolment and subsequent verification and identification events - and ensuring these externalities are accounted for and 'trained into' process and understanding is crucial in order to manage them.

For the purposes of this guidance, we break these 'failure modes' down into two key categories. The first is largely technical - factors which may impact the ability to acquire high-quality biometric data in the first place, and in the absence of which

there may be a Failure to Acquire - and issues with identification or enrolment. The second is the human - which may also precipitate these failure modes, but crucially may be the critical path between exception handling which ensures inclusive, fair rollout, and exclusion problems or significant distress/harm.

## Environmental and Technical Factors

Environmental and technical factors tend largely to derive from the physical environment in which capture takes place. For instance, humidity, dust, or debris which obscures the working surface of a finger sensor or the lens of a camera will clearly prevent effective capture of an image - while damage to the sensor or phone may prevent the device from functioning.

Where using hardware-based biometrics, the hardware itself may be more or less able to cope with these factors. Sensors and extraction algorithms may not have been designed for low-light, high-dust environments; or tested with darker skin tones.

Coping with these factors requires three things - firstly, an anticipation of the factors likely to arise in the operating context. Some of these may be unique to the context, but some can be predicted. For instance, across contexts where humanitarian development programming takes place, hardware (potentially including phone and capture device) may need to operate:

- In temperatures from freezing to ~40C or more outdoors or in direct sunlight to cope with seasonal variations, depending on the continent and operating context;
- In heavy rain or moisture which requires a waterproof rating;
- Where the sensor or finger is dirty, greasy, or obstructs a perfect capture;
- Without reliable power for hours or days;
- With tolerable accuracy given the lighting conditions and ethnicity of the subject;
- In rough conditions, likely to damage wires or fragile components (i.e. it may need to be wireless and suitably impact-tested);

For safety reasons, it is also likely to need to have passed a variety of safety tests such as those defined in EN 62368-1:2014 for safety to end-users.

Some of these factors will be difficult to address if not considered during procurement - but they should also be factored into the deployment. Physical sites, training for users, deployment timing, will need to consider the likelihood of encountering these factors.

## Adjudication and Exception Handling

Even where environmental and other conditions are planned for, humans will need to be trained to negate them - for instance, by keeping equipment out of direct sunlight, wiping down the sensor, encouraging subjects to clean hands before placing fingers on the sensor, or choosing appropriate sites which allow shelter from heat, rain, or wind.

But beyond these circumstances, user behavior will also impact effectiveness of the solution. This handbook has already discussed at length the impact which ***thresholds*** will have if incorrectly set.

### *Planning for failure*

Thresholds may vary substantially based on environmental conditions and the characteristics of the subject(s), requiring the process of calibrating and setting the threshold which consider these conditions during the rollout of the project.

Even where this is undertaken well and at the right level of granularity, biometrics are inherently probabilistic - some proportion of users will *always*

be falsely rejected (or accepted) - or prevent a high score which requires manual decision-making - even if this proportion is 1 for every thousand successful events.

Where the solution is running in 'identification' mode in particular, this may require that a user perform a step called **adjudication** to manually delineate between possible matches. This may be done based on alternative documents, biographic data, photographs, or even prompt for a re-authentication event.

Users *must* be trained to handle these exceptions - with clear workflows which consider the possibility of false rejection or acceptance. These workflows should prompt users to consider the adjudication step where necessary, as well as compassionately following an **exception-handling** process in particular in instances where a false rejection may cause significant disbenefit or harm to the subject - for instance, denying access to resources or services.

In these circumstances, clear workflows at point of capture may also need to be supplemented by helpdesks, alternative contact mechanisms, or other channels which allow users to express concerns or provide feedback where issues could be systemic.
Consider in particular exception-handling workflow, training for users, and complaint mechanisms which consider at a minimum failures:

- **Pre- and During Enrolment** - i.e. where users may initially be turned away if the biometric collection (or some other factor) causes a failed enrolment. Workflows must account for this - as well as the likelihood and logistics of re-enrolment in instances where a user requires a follow-up enrolment or re-enrolment;
- **During identification/verification** once enrolled - i.e. during routine transactions for balance-checking, top-ups, individual engagement, or other individual interactions with subjects or proxies. What happens when it goes wrong? Can family members safely act on vulnerable users' behalf? Is there an exception-handling process if the biometric fails entirely? How can users express concerns or feedback?
- **During distribution/intervention** together or separately from the biometric event itself. Will participants ever suffer physical, emotional, economic, or other consequences if a system failure, authentication, or authorization event suggests or prompts a decision not to permit a user to proceed. Is there a manual process for review, re-enrolment, distribution without ID, or otherwise ensuring no subject has cause to lose out or be harmed?
- **After the fact** - for instance, where community members express concerns later regarding a perceived loss, disinclusion, not having been present during a service delivery window, how data is used, or some other matter. It may be necessary to train (and signpost to) non service-delivery staff to comprehensively 'hear' concerns beyond individual transactions.

### *Reducing the Likelihood of Failure*

Even once exception handling mechanisms are put in place and environmental factors are considered, various aspects of user behaviour may influence the likelihood of a failure to acquire, enrol, or successfully capture data. These will vary by modality and should be subject to testing and consideration with the vendor. But there are some common factors it is worth considering.

For finger or hand-based biometrics - or other modalities with sensors, such as eye, iris, or palm vein - placement of the digit, body part, or face near or in a sensor may be critical. Some solutions may offer real-time feedback on placement of a finger, or a mechanical solution such as a physical guide for hands or face.

But users are likely to need training on **placement** on sensors, as well as **pressure** where the modality is not contactless. Where a solution does not provide feedback on these factors (e.g. via LEDs or in-app feedback), regular assessment may be needed - linking performance at user level to accuracy data - and re-training where needed.

Beyond purely functional considerations, users will also require training on selection of digits hands, or other factors where biometrics are multi-modal or include multiple capture 'moments'.

Even where data is highly accurate, we have touched already on the various factors impacting understanding and risk to participants - emphasising the importance of transparency, contextualisation, and communication.

It is critical that users are trained to **contextualise and discuss how data is used** - even where in-app prompts, text, recordings, or other digital tools are used (and even if there are other ways users are communicated with). The conversation at point of capture will for many subjects be the primary mechanism for enabling understanding, and if handled uncompassionately may produce distress, high rejection rates, and low compliance with instructions.

All of these factors may require **incentives** and **ongoing monitoring** - consider how users are incentivised and if, for instance, poorly-considered performance-based targets (e.g. # of registrations in a day) may mis-incentivise or reduce the likelihood of success. Consider monitoring and providing regular feedback on complaints, accuracy, and other metrics - and incentivising on the basis of acceptance and feedback as well as volume or throughput.

## Accountability & Transparency

We have covered some of these points already e.g. when talking about consultation, informed consent, and other types of inclusion issue - but outline here some suggested forms of good practice around accountability to an affected population when working with their biometrics.

## Program Modalities

Whilst much of this guidance considers elements of biometric safety which apply ubiquitously across various types of humanitarian and development intervention, there are some nuances specific to distinct types of intervention.

### Humanitarian Interventions

Humanitarian interventions, characterized in particular by short deployment cycles and potentially more vulnerable cohorts of participants, are in many ways the 'hardest' use-case, requiring the most preparation but allowing for minimal planning and execution time.

During a response, life-saving assistance may need to be delivered over a timeframe of hours and days, negating the ability to carry out many iterative cycles of planning, execution, checking, and review.

Humanitarian actors will also need to have undertaken needs/benefit assessment, security review, context analysis, and potentially other steps in advance of deployment - some of which are suggested in Appedix - Skills & Responsabilities.

Humanitarian users will need to consider which of these steps can be carried out in advance, and are sufficient to 'greenlight' incorporation of biometrics

into a humanitarian toolkit, as well as which elements need greater or nuanced consideration given the inclusion of biometrics as compared for instance to a standard data collection, manual, paper voucher-based, or other activity.

Some of these steps cannot be universalised. Humanitarian biometrics deployments therefore must be well-integrated into deployments able to assess the context in line with this guidance to undertake a balanced risk assessment; in particular considering the needs of the affected population and factors such as theft, reuse, and seizure of data by parties to conflict or other threat actors in the humanitarian environment.

When considering how to 'greenlight' humanitarian biometrics, users will also need to consider which specific technical safeguards are the right ones for them. In particular, users should consider which Template Protection schemes, cryptographic techniques, storage approaches, and other Privacy Preserving Techniques or safeguards such as Fully Homomorphic Encryption are applicable and will best-meet their needs or threat model.

Fully considering which of these are right goes well beyond this guidance, but across the humanitarian ecosystem there are increasing uses of (and mandates for) these techniques in particular within the Red Cross and Red Crescent Movement[42][43] as well as in-depth academic research and exploratory work[44] - and users should consider carefully if their needs can be met without a mixture of them.

Finally, particularly in an age of complex environmental, economic, political and social problems, humanitarian interventions may begin in a hurry, but are often multi-year, multi-agency endeavours with developments, referrals, and evolution which cannot simply be anticipated at the outset. Collection of data in these contexts therefore requires particular vigilance regarding the likelihood for the legitimate need to reuse data as well the dangers of scope creep which strains at the good practices of purpose limitation and transparency.

## In-kind Distributions

Where using biometrics for programming which may involve a significant and life-changing disadvantage in the event of a false negative or false positive - e.g. a genuine service recipient who is turned away, or a fraudulent subject who is able to access goods - greater consideration must be given to mitigating these potential disadvantages. Significant consideration has been given to the sources of some of these in terms of accuracy throughout this guidance; users deploying biometrics for these distributions or interventions will need to carefully consider:

1. How accuracy is measured and established;
2. What alternative pathways are available in the technology in use (e.g. troubleshooting processes, ability to reissue of cards biometrics, manual overrides or faultfinding processes at distribution points) to reduce the impact where inevitably exceptions happen;
3. What investment and access is needed - and for instance whether unattended biometrics or disbursed Points of Sale or Distribution without a helpdesk or accountability mechanism are feasible;
4. Monitoring carefully for perception of as well

42 IFRC (14/12/2021), Digital Identity: An analysis for the Humanitarian Sector
43 ICRC (28/8/2019), Policy on the Processing of Biometric Data by the ICRC
44 Sukaitis, Justinas (15/04/2021), Building a path towards responsible use of Biometrics

as actual disbenefit as the result of any loss of access or refusal.

## Health

While health may in many instances be similar to a distribution activity, health use-cases often involve longer-term retention of data, and may involve sharing and storage across the lifetime of participants, as well as sharing with government health authorities, health providers, or research authorities.

In these cases implementors should apply particular thought to the Informed Consent process in use - in particular how data collection interleaves with processes which may be necessary to satisfy medical ethics or research requirements, and whether diagnostic, research, or continuity of care use-cases are sufficiently well communicated to subjects.

The longevity and transfer of health-linked data (i.e. the length of retention periods, and likelihood that data will be transferred to other clinical or research providers) should also be factored into risk assessment early on in the design process. In volatile contexts or states with no or low-maturity national legal frameworks, consideration should be given in program planning to incorporating reassessment of the context and risks to data intermittently; for instance, providers may wish to reconsider how transfer of power or political change may affect the way data is used, or how changes to the structure of government or legislation introduce or remediate risks.

## Cash

Whilst sharing in principle many of the challenges of in-kind and health use, cash distribution often incorporates more porous integrations with Financial Service Providers such as banks, mobile money platforms, and government - transferring data to third parties once enrolment has taken place, exchanging data when making disbursements, etc.

Movement of money is generally also subject to requirements such as KYC and Aid Diversion - meeting needs to prevent money laundering and criminality, reduce fraud and meet the needs of funders regarding effective use of government funds, or satisfy other security requirements.

These requirements can be challenging and inflexible - and in many national contexts will have exceptions in the law requiring, permitting (or safeguarding) transfer of data. The relationship between users and governments or regulators can also be such that requests or requirements for data can be challenging in practice to understand or refuse[45].

Biometrics in programming such as this can also be tempting to mandate or require to satisfy Aid Diversion requirements. Biometrics are indeed a powerful tool for preventing fraud, but their use purely for this purpose should nonetheless consider the issues of equity and fairness treated throughout this guidance, as well as being backed by evidence and provide clear benefit to the affected population which is communicable. Truly responsible usage must reflect these principles even where the ‘purpose’ is largely one of risk reduction.

45 Raftree, Linda / CaLP (2021) - Case Study: Responsible Data Sharing with Governments

**Warning** - These complexities and nuances can be challenging to map and understand. Program teams should consider what access, capacity and capability is needed to do so before committing to work which may become challenging to safeguard

Consideration of these complex dataflows and requirements must be part of program design, which should treat:

1. Mapping of the dataflows between FSPs, Government, and Others;
2. Clear understanding of the roles of these parties - including the Controller identity and accountabilities;
3. Consideration before committing to any deployment whether pre-existing solutions or systems (e.g. FSP networks, Government Social Security tools or other digital systems) may be better to reuse or iterate or negate the need for deployment of biometrics or other tools;
4. Where biometrics are in use for fraud prevention or other risk-reduction, how this usage is evidenced and justified;
5. Risk assessment of the impacts of these dataflows to subjects;
6. Consideration of the possibility for any future development of 'externalities' such as financial regulation, further requests for data, or government seizure;
7. Communication of the flows, responsibilities, benefits, and impacts as part of the enrolment and implementation of the program;
8. Consideration of any critical risk factors which may make any of these steps impossible in practice and may (or should) halt implementation or design.

## Interoperability, Nexus, and Transition to Development

Increasingly, data is collected in interoperable formats and systems designed to allow reuse, referral, and reduce the burden on participants of collection & use. Huge opportunity for inclusion, long-term alleviation of poverty, improvement of health outcomes, and other SDG-aligned work may be unlocked by integrating systems and allowing a smooth transition, for instance, from humanitarian food distribution into long-term economic justice programming - inevitably including the sharing of data.

This type of work often - and increasingly - brings about:

1. Greater movement and transfer of data between separate organisations and across geographic and legal boundaries;
2. The use of data for additional, complementary, and separate purposes.

Transfer can often be contentious or sensitive - in particular where it may not be clear to participants or give rise to expensive re-consent or re-communication exercises or the need to undertake due diligence between partners.

Where use-cases are dissimilar, it may also be that the Purpose of reuse - however noble - will not have been clear to subjects, and may be incompatible.

These challenges and tensions are deeply treated in legal frameworks, and while the full depth cannot by necessity be covered here, practitioners should be mindful that they exist - and factor them into planning and decision-making both during design and at moments of change.

Interoperability considerations also have significant bearing on storage (as outlined elsewhere in this guidance some storage types will bring interoperability challenges), transparency (systems with the potential for reuse or data sharing will require a different approach to communicating how data is used to subjects), and potentially technical considerations such as the lawful basis.

## Monitoring & Evaluation

Throughout this guidance, we have signposted to areas of the design and deployment process which benefit from or require learning loops, evaluation, and structured research in order to enable a safe approach.

**Warning** - Without meaningfully asking the right questions as part of the monitoring, evaluation, and accountability practice embedded into a biometrically-enabled program, it is unlikely that the biometric capture can sustainably and enduringly be done safely and respectfully

While the MEAL plan for a project must be considered in the light of the program's unique challenges and deliverables, there are a few key stages at which practice is likely to be needed, whatever the activity - we break them here down into pre-deployment (Piloting + Evaluation), during deployment (Bias + Equity; Perception + Harms), and Overall Effectiveness.

### Piloting + Evaluation

During initial piloting and testing with the target population - in particular where the use-case is new or unexpected - we suggest that qualitative research and feedback collection regarding the perception the user has towards biometrics should be undertaken prior to mass roll-out - as well as any technical, people, or procedural issues.

Questions that interventions may consider include:

- How did you feel about the process of collecting your data using the tool?
- Were you registered quickly and without problems?
- What did you understand about how your data would be used?
- Would you be comfortable with another family member being biometrically enrolled?
- Were any of your concerns unanswered during enrolment?
- How safe did you feel during enrolment and about the data collection process?

Where an intervention has specific tension points, questions, focal group discussion, or inquiry into these tension points should also be considered - informed by the risk assessment and context of the project.

Where a PIA or similar exercise is being carried it out, it is likely to be desirable to integrate research

into the 'consultation' process carried out as part of its delivery.

This exercise of inquiry should then be able to feedback into the design and deployment, informing training, physical design choices, or other aspects of program design and delivery.

### Bias and Equity

Once a deployment is underway, it is likely to be necessary to monitor any equity, bias, or inclusion issues which may arise during the project.

These could include quantitative data on Accuracy or FTA issues - which may be reported automatically via technical tools or monitored in real-time.

They may also include qualitative data from feedback or complaint processes, collected via rejection workflows within the app, feedback from users of the system (including their perception and satisfaction with the tool), as well as focused inquiry where applicable.

### Perception and Harms

Ongoing monitoring and engagement with affected communities should not just include technical assessment of accuracy and acquisition of data, but also the perception of how data is used - as well as any disengagement, distress, or unease amongst the community.

These may be gathered individually, via community-based work, as well as informally via users and others.

As well as perception and distress, serious consideration should be given to any harms or perceived harms precipitated by the intervention, sharing of data, or failure mode of the biometric component.
This data should regularly be fed back into the program design.

### Overall Effectiveness

When the intervention has been completed, MEAL should consider the overall effectiveness of the solution - including any technical, teething, inclusion, training, or other issues as outlined throughout this document.

This may also link back to the need/benefit analysis undertaken as part of the biometric deployment, which may link directly to the overarching program and impact design.

## Organisational-wide competence, governance, and policy

Finally, the step many implementors can - and should - start with; thinking about organisational governance of responsible biometrics. For many, the root of their practice will inevitably begin with established Data Protection, Responsible Data, Cybersecurity, or other policy and work areas, and complementary training and support offered to staff and implementation teams.

Yet as we have established throughout this guide, Biometric technology is nuanced, and while it shares deep similarities with other forms of data collection - any of which can be harmful if subject to maladministration - it has unique and specific failure modes, safeguards, and properties. Organisations will wish prior to deployment to establish the right red lines, governance, overarching policy, and training that enable them to make the right safe steps for them.

Organisational policy is likely to need to consider:

- Any overlaps with other policy areas;
- Whether or not a decision has been made on the use of this technology at all;
- Key responsibilities for deployment, decision-making, and risk assessment;
- Key risk areas, controls, or connections with the organisation's own work;
- The implementation plan for the policy, and where support can be sought;
- Other policy lines based on structured content from this guide, good practice, peer policy, and organizations' own experience.

There are many examples of organisational policy and critical guidance which organisations will wish to draw from, including ICRC[46], Oxfam[4748], The Engine Room[49], UNHCR[50], UNICEF[51], the Biometric Institute[52], and others.

**But overarchingly, and whatever an organisation's appetite for risk, style, policy framework, a mindful approach which puts people at the center of consultation, choice, risk assessment, and need/benefit analysis, is cogniscent of the state of the art in protective safeguards from the ordinary to the exotic, makes governed and documented decisions which are rooted in an understanding of the context, potential for change, potential for misuse or error, and which remains cautious, curious, and inquiring will maximise the changes of success - in making meaningful social impact on the world around us, while limiting the likelihood of doing harm.**

46 ICRC (2019) - Biometrics Policy, accessed at https://www.icrc.org/en/document/icrc-biometrics-policy
47 Oxfam (2021) - Biometric & Foundational Identity Policy, accessed at https://oxfam.app.box.com/v/OxfamBiometricPolicy
48 Oxfam/The Engine Room (2018) - Biometrics in the Humanitarian Sector, accessed at https://www.theengineroom.org/wp-content/uploads/2018/03/Engine-Room-Oxfam-Biometrics-Review.pdf
49 The Engine Room (TBC) - Biometrics in the Humanitarian Sector
50 UNHCR (2022) - Guidance on Registration and Identity Management, accessed at https://www.unhcr.org/registration-guidance/
51 UNICEF (2019) - Faces, Fingerprints & Feet, accessed at https://data.unicef.org/wp-content/uploads/2019/10/Biometrics_guidance_document_faces_fingersprint_feet-July-2019.pdf
52 Biometrics Institute (2020) - Good Practice Framework, accessed at https://www.biometricsinstitute.org/biometrics-institute-good-practice-framework/

## Appendix - Responsibilities, Lifecycle, Skills

| Index | Key Step | Who may be Responsible and where? | Skills Required | Design + Implementation Considerations | Notes |
|---|---|---|---|---|---|
| 1 | **Organisations should implement an overarching Policy guiding adoption of ethical principles of deployment.** | Organisation - Any entity making use of biometrics. | Data Protection, Biometric Expertise, Programmatic Risk, Cybersecurity, Compliance, Organisational change. | Organisations should both implement a policy and ensure it is appropriately embedded in key teams prior to considering deploying biometrics in their work. | Various organisations have previously published policies on Biometrics which organisation may make use of as guidance[53][54].<br><br>This table is also suggested as a framing for organisations in considering key policy lines and competencies. |
| 2 | **Organisations should train their staff on implementation of the biometric policy + broader data ethics or privacy policies and principles - including any relevant skills.** | | | | |
| 3 | **Impementors should craft a clear problem statement outlining their intended use of biometrics.** | Project - Entity responsible for implementation. | Technology for Development, Compliance, Organisational change. | Crafting a problem statement must form part of project design, and may need to synthesise the expectations and intent of multiple entities - including the donor and implementor. | |
| 4 | **Implementors should understand whether biometrics are a good fit for the project.** | Project - Entity responsible for implementation.<br><br>Biometric Vendor / Partner. | Technology for Development, Biometric Expertise, Compliance, Business Analysis, Organisational change. | Matching the solution and understanding the expected benefit can be nuanced and where organisations do not have in-house knowledge they may consider outsourcing assessment or bringing in specialist support. | Organisations should consider more broadly documenting and assessing these 'pre-deployment' phases as part of subsequent research and learning, particularly where deploying biometrics in under-researched use-cases. |
| 5 | **Implementors should undertake a Needs & Benefit Assessment.** | Project - Entity responsible for implementation. | Technology for Development, Biometric Expertise, Compliance, Business Analysis, Program Design. | As part of the program design, implementors should build on the 'fit' of the tool, and assess the benefit to subjects as well as the organizational need - balancing them as part of a structured decision-making process before moving into deployment or procurement. | |

53 Oxfam (2021) - Biometric and Foundational Identity Policy

54 ICRC (2019) - Policy on the Processing of Biometric Data

| | | | | | |
|---|---|---|---|---|---|
| 6 | **Implementors should Identify the right modality, partner, and technology for their needs based on foundational analysis of them. This should include appropriate PPTs, Cryptsystems, or use of technologies such as FHE and BTP.** | Project - Entity responsible for implementation. | Technology for Development, Data Protection, Cyber Security, Biometric Expertise, Compliance, Business Analysis, Program Design. | While organisations may offer a 'portfolio' of tools which undertake this analysis globally, there may also be instances where 'matching' of the tools and partners to the project are needed. | Implementors should consider carefully whether RfP responses, project plans, and budgets include the right timeframe, tools, skills, and funding to undertake these steps. |
| 7 | **Implementors should Identify any accuracy challenges or other confounding issues with biometrics for individual deployments as part of the deployment process.** | Project - Entity responsible for implementation.<br><br>Project - Biometric Vendor / Partner.<br><br>Portfolio - Implementor while onboarding tools. | Technology for Development, Biometric Expertise, Compliance, Business Analysis, Program Design. | This analysis and understanding is likely to require detailed experience with biometrics, and implementors may be well-advised to engage a specialist where they do not have biometric expertise in-house. | |
| 8 | **Implementors should assess the context into which biometric or identity tools are deployed, considering any relevant factors which inform the design and risk management.** | Project - Entity responsible for implementation.<br><br>Project / Context - Donor / Implementing Partners. | Technology for Development, Biometric Expertise, Compliance, Business Analysis, Data Protection, Cyber Security, Protection. | This analysis will be best-done in tandem with protection, conflict, and other context analysis undertaken programmatically - but including digital, data, and other elements relevant to individuals' understanding of biometrics and contextual factors which may cause them harm. | |
| 9 | **Implementors should define and map their relationship with each other, and relevant safeguards.** | Various - All Implementing or Supporting Partners.<br><br>Portfolio - Implementor while onboarding tools or partnerships. | Technology for Development, Biometric Expertise, Compliance, Business Analysis, Data Protection, Cyber Security, Protection. | Mapping responsibilities is likely to be a precursor to signing MoUs, implementation agreements, DPAs, or other contracts. | |
| 10 | **Implementors should ensure their approaches to ethics safety are sufficiently aligned, and undertake relevant due diligence of each others' approaches.** | | | Alignment and Due Diligence is likely to be undertaken prior to design or in the early stages of partnership. In highly structured partnerships, this may be an audit or capacity assessment process - but may include review of Information Security, Data Protection, System Design and Architecture, or other documentation, cryptographic design, PIAs, or other technical literature, or even involve third party review. | Some considerations regarding due diligence and assurance are given in Appendix - Due Diligence and Safety Tools. |

| | | | | | |
|---|---|---|---|---|---|
| 11 | **Implementors should map out the dataflow of their project throughout its lifecycle as part of the design process.** | Project - Entity responsible for implementation. | Business Analysis, Technology for Development, Data Protection, Technology. | It is almost impossible to responsibly design a project or undertake risk assessment without a dataflow - a map of where data goes, which systems it resides in, and which partners will access it. | |
| 12 | **Implementors should map out the threats they expect their tools and intervention to face, and identify suitable safeguards based on those anticipated threats and threat actors.** | Project - Entity responsible for implementation.<br><br>Portfolio - Implementor while onboarding tools.<br><br>Project / Context - Donor / Implementing Partners. | Business Analysis, Technology for Development, Cyber Security, Risk Assessment. | Based on context and dataflow, organisations should make use of an appropriate approach for identifying threats. This may be done in one or various places - project, country, endeavour, or international level. Where a specific project is highly risky or complex it is likely that threat modeling at the level of project or operating context will be needed. | Further notes are given elsewhere in this implementation on guide on some of the available options. |
| 13 | **Implementors should understand the Purpose of data use and any challenges or limitations deriving from or linked to adhering to this Purpose.** | Project - Entity responsible for implementation. | Business Analysis, Technology for Development, Data Protection, Risk Assessment. | The Purpose should be understood in the context of its role as a privacy safeguard, but also given knowledge of the operating context and any constraints - either on future project work if a purpose is not captured sufficiently, or on the ability to 'stick to the red lines' e.g. given tensions around data sharing. | Robustly understanding the purpose and identifying the right lawful basis will be heavily contingent on robust planning, stakeholder engagement, and data flow mapping. Without these other foundational steps, Purpose may be elusive. |
| 14 | **Implementors should identify a Lawful Basis and root their choice in an understanding of individual experience, choice, and power.** | Project - Entity responsible for implementation. | Data Protection, Legal. | Done intersectionality and thoughtfully, the choice of lawful basis should be the crown jewel of organisational accountability and agency - providing a 'north star' for the approach to consent and transparency, with its roots in purpose.<br><br>Homogenous interventions may share a lawful basis which is 'standardised' across projects - but some projects may require specific legal analysis. | |

| | | | | | |
|---|---|---|---|---|---|
| 15 | **Implementors should complete suitable risk assessment and Privacy Impact Assessment to support safe data use in their project - including matching the use of any PPT or other protective technology with the risks in the target operating space.** | Project - Entity responsible for implementation. | Data Protection, Legal, Business Analysis, Technology for Development, Cyber Security, Protection, Risk Analysis. | A PIA may not be legally required for all projects, but any project should implement a suitable risk assessment whether or not it takes the form of a PIA. Where projects are complex and multi-stakeholder - or the role of the donor, implementor, and partners is unclear - the home for this analysis and roles of the various partners in collaborating - as well as owning the subsequent risk mitigations and resourcing their resolution - should be carefully considered when designing the project and considering partnership roles. | Detailed guidance is given elsewhere in this guidance on where risk assessment may live, the relationship between risk assessment and privacy impact assessment, and some of the suggested 'minimum criteria' for undertaking it well. |
| 16 | **Implementors should undertake an appropriate Informed Consent programme, offering layered and suitable forms of transparency information, choice, and broader sensitisation and engagement.** | Project - Entity responsible for implementation.<br><br>Project - Implementing Partners. | Data Protection, Legal, Business Analysis, Technology for Development, MEAL, Inclusive Design, Protection, Risk Analysis. | How a community is consulted, informed, and offered choice is a difficult and potentially multi-stage process. Projects should carefully consider not just the Design of this process, but also how it is evaluated and iterated.<br><br>It should span not just the 'moment of consent' but also the broader consultation of communities during design and setup, and interleave with the solution, any PIA consultation undertaken, and broader accountability and inclusion practice.<br><br>It should also include the broader consultation of civil society - for instance on attitudes towards data collection, safety, and identity systems. | Integrated planning of the 'full picture' of consultation, engagement, feedback, and evaluation will yield the most benefit throughout the lifespan of the project, ensuring it remains human centric beyond design and throughout the lifecycle of implementation and subsequent evaluation. |
| 17 | **Implementors should undertake appropriate consultation with the affected community during implementation of biometric solutions** | Project - Entity responsible for implementation.<br><br>Project - Implementing Partners. | Data Protection, Legal, Business Analysis, Technology for Development, MEAL, Inclusive Design, Protection, Risk Analysis. | | |
| 18 | **Implementations should undertake appropriate consultation with civil society groups during design and implementation of biometric solutions.** | Project - Entity responsible for implementation.<br><br>Project - Implementing Partners. | Data Protection, Legal, Business Analysis, Technology for Development, MEAL, Inclusive Design, Protection, Risk Analysis. | | |

| | | | | | |
|---|---|---|---|---|---|
| **19** | **Implementations should provide appropriate channels for feedback and complaints - making it clear the various forms of request which can be made.** | Project - Entity responsible for implementation.<br><br>Project - Implementing Partners. | Data Protection, Legal, Business Analysis, Technology for Development, MEAL, Inclusive Design, Protection, Risk Analysis. | Without considering how, when, and where participants may be able to do this, it is unlikely valuable feedback regarding equity or inclusion issues will be identified in a timely manner.<br><br>Channels should advertise the Rights and pathway available - including breach reporting, DSRs, and broader complaints. | |
| **20** | **Implementors should conduct pilot phases before scaling up to broader interventions, testing any aspects of the privacy lifecycle necessary to 'stress test' the final design.** | Project - Entity responsible for implementation.<br><br>Project - Implementing Partners. | Data Protection, Legal, Business Analysis, Technology for Development, MEAL, Inclusive Design, Protection, Risk Analysis. | Undertaking smaller-scale deployments which are more closely monitored reduces the likelihood that equity and inclusion issues will propagate into scale-up - but may require budgeting and incorporation into project plans and RfPs. | |
| **21** | **Implementors must make appropriate pathways available to handle Data Subject requests (access, deconsent).** | Project - Entity responsible for implementation.<br><br>Project - Implementing Partners. | Data Protection, Legal, Business Analysis, Technology for Development, MEAL, Inclusive Design, Protection, Risk Analysis. | In addition to advertising and making available channels for expressing concerns or requesting data, deconsenting, etc - organisations must also have pathways in place to handle these requests when they do arise. This may mean providing appropriate training to field staff, sufficient language coverage, or other logistical issues. | These foundational components of Data Protection practice (which may be predisposed by organisations' compliance and cybersecurity programs) should be carefully considered in the light of the context and it's challenges & limitations. |
| **22** | **Implementors must implement appropriate processes for handling complaints or concerns from subjects.** | | | | |
| **23** | **Implementors must implement appropriate processes for responding to notifications by individuals or others of any potential breach.** | | | | |
| **24** | **Partners must implement appropriate processes for notifying counterparts regarding Incidents or Breaches.** | Project - Entity responsible for implementation.<br><br>Project - Implementing Partners. | Data Protection, Legal, Technology for Development, Protection, Risk Analysis. | Without preparation it is rare that breach notification is timely. Ensuring that MoUs or contracts define counterparts, reporting times, and pathways will help ensure that if a critical incident occurs, the right thing happens. | |

| | | | | | |
|---|---|---|---|---|---|
| 25 | **Implementors must implement appropriate processes for detecting and responding to breaches.** | Project - Entity responsible for implementation.<br><br>Project - Implementing Partners. | Data Protection, Legal, Business Analysis, Cybersecurity Technology for Development, Protection, Risk Analysis. | Whether technical, procedural, or otherwise, preparation is also necessary to ensure breaches can be detected and responded to. While standard IT lifecycles and data protection programmes sometimes include some of this preparation, project teams should consider what is not included, and what processes, safeguards, or practices specific to their project might be necessary.<br><br>Where provision cannot be made for detection, handling, or notification - projects may wish to consider in their risk assessments whether the project is safe or needs design changes to be implementable. | |
| 26 | **Implementors must have the ability to communicate with affected subjects in the event of a breach or incident.** | Project - Entity responsible for implementation.<br><br>Project - Implementing Partners. | Data Protection, Legal, Business Analysis, Cybersecurity Technology for Development, Protection, Risk Analysis. | | |
| 27 | **Data sharing must be governed, defined, and contracted-for.** | | Data Protection, Legal, Business Analysis, Cybersecurity. | Almost any data sharing relationship which is not highly unusual and single-instance is likely to need contractual governance and further analysis. Making mapping these relationships out part of a dataflow analysis and risk analysis early in a project will minimise disruption later on. | |

| | | | | | |
|---|---|---|---|---|---|
| 28 | **Implementors must have a plan for data disposal.** | | Technology for Development, Data Protection. | Project design and risk assessment must include the circumstances and execution of data disposal at the end of a project. | These aspects of lifecycle and change management are frequently forgotten, omitted from project plans, or have unclear responsibility. Ensuring they are well governed and owned will maximise the likelihood that they are done well. |
| 29 | **Implementors must re-assess the context in the event of any significant change.** | | Data Protection, Legal, Business Analysis, Cybersecurity Technology for Development, Protection, Risk Analysis. | Projects must incorporate triggers and designated responsibility for reassessment during changes of context, to the partnerships in a project, in the event of a change to the architecture of the dataflow, or in the event of any other change which could impact individuals. | |
| 30 | **Implementors must re-assess the project risks in the event of any significant change to the project scope or deliverables.** | | Data Protection, Legal, Business Analysis, Cybersecurity Technology for Development, Protection, Risk Analysis. | | |

## Appendix - Due Diligence and Safety Tools

| | DPA | TIA | Policy DD | Review / Require Certification | Pentest (ask) | Pentest (commission) | Responsibility Matrix | Audit | Values Alignment | MoU / other article |
|---|---|---|---|---|---|---|---|---|---|---|
| **Simple** | Yes | Potentially | Yes | More likely | Yes | Potentially | Less Likely | Potentially | Unlikely | Unlikely |
| **Integrated** | Potentially | Potentially | Potentially | Potentially | Less likely | More likely | More likely | Potentially | Potentially | Potentially |
| **Complex** | Less likely | Less likely | Potentially | Potentially | Less likely | More likely | More likely | Less likely | More likely | More likely |

## Appendix - Vocabulary & Key Definitions

| | |
|---|---|
| **1:1** | 1:1 matching, or Verification, is a modality of deployment which uses biometric data alongside a hypothesis or knowledge of the individual - for instance a presented ID card with the name - and therefore compares a biometric probe from the subject with one record to ascertain their identity. |
| **1:N** | 1:N, 1:Many, or Identification, is a modality of deployment which uses the biometric data itself to search a gallery of records to establish the identity of a human by linking to other data directly using their biometric data. |
| **Accuracy** | The Accuracy of a deployment can be measured in a variety of ways, but will correspond to some metric regarding the number of instances a match cannot be made, is made incorrectly, or a valid user is unmatched. |
| **Adjudication** | Adjudication is the process by which a human or automated process makes a decision about identity probabilistically (for instance based on a match score) and/or using other data (for instance, comparing the record with ID documents). |
| **Anti-Spoofing** | Anti-Spoofing features prevent an attacker who is attempting to present fake or reused biometric credentials in order to impersonate another user. |
| **Attendant** | Attendants are the humans who use or operate biometric hardware and software and have a supervisory role, ensuring hardware is used correctly, and potentially carrying out other tasks such as adjudication, fraud prevention, or maintenance. |
| **Biometric data** | Biometric data is data which derives from measurement or observation of human behaviour or physiology, and is used for the identification of that human through analysis and comparison with future behaviour and/or physiology. |
| **Cancellability** | See renewability |
| **Confidentiality** | Confidentiality is generally presented as one of the three core goals of Information Security - alongside Integrity and Availability. The Confidentiality of data is the quality of being available only to authorised and intended users and recipients, a quality sustained through technical and other safeguards, or 'controls', implemented as part of an Information Security lifecycle. |
| **Consent** | Consent can be understood ethically as a process by which an individual accepts an intervention or use of data based on knowledge of the activity and its potential effects on them, and specifically in Data Protection law as a Lawful Basis rooted in individual choice and with specific requirements where it is the pathway used to collect or make use of data. Ethical Consent and Consent as a lawful basis do not necessarily need to co-exist; an activity obtaining Ethical Consent may use an alternative lawful basis to Consent. |
| **Data Subject** | The Data Subject is the individual to whom Data relates and who can be linked to it. In the context of Biometric Data, they will be the individual the data was collected from. |
| **Deduplication** | Deduplication is the process of removing records in a dataset which relate to the same person and eliminating all but the 'master' record (or combining the records together) to produce a unique dataset. |
| **Encryption** | Encryption is a process which transforms input data - usually referred to as Plaintext - into an output which is encoded in a manner designed to be unusable to anyone other than the intended recipient or user, generally using a Key which is required for the use of the data. Various types of Encryption exist, and while consumer use-cases often distinguish between data encrypted while being moved ('in transit') and stored ('at rest'), the management of Keys and variety of techniques and shortcomings make the real-world security and privacy protection offered by Encryption varied, and intrinsically based on the circumstances and application in question. |

| | |
|---|---|
| **Enrolment** | Enrolment is the process by which a subject is initially registered into a biometric database, typically capturing their biometric data for storage alongside other programmatic data such as name or identity. |
| **False Acceptance** | False Acceptance is the identification by a biometric system of a subject who is not the intended subject, for instance allowing Person B to access Person A's biometrically-authenticated bank account. |
| **False Rejection** | False Rejection is the rejection of a subject who should have been allowed to pass by an authorisation or authentication process. For instance, if Person A attempts to log into their online bank account but has dusty fingers and the biometric authentication process fails to identify them, this may be a 'false rejection'. |
| **Feature Extraction** | Feature Extraction is the process within a biometric system through which the key components of a biometric factor which are used to undertake a comparison are extracted. In the case of a fingerprint these may be the loops and whirls of the fingerprint whilst other modalities will work differently. |
| **Foundational Identity** | Foundational Identity systems are platforms built for long-term use, potentially across multiple use-cases. For instance, a government digital identity system. |
| **Functional Identity** | Functional Identity systems are generally integrated into specific interventions (for instance an NGO's food distribution program in a refugee camp), leveraging identity for a single or set of homogenous use-cases, often with no intention to use the data long-term. |
| **Gallery** | The Gallery is the term within a biometric system for a database of biometric records against which comparisons are made, for instance in a 1:N or Identification 'search' event. |
| **Identification** | See 1:N |
| **Identity System** | An Identity System is a digital system which holds data regarding a number of people, including the means to ascertain that a physically present or digitally engaged subject is the human in a particular record, who may be seeking to pay, access services, or carry out some other function. It is typically designed to enable 'authentication' and 'authorization' functions in order to prevent fraud, facilitate access, uphold the role of law, etc. |
| **Implementor** | An Implementor is the party who is undertaking work to build or commission a biometric system. They may or may not be the funder, controller, or accountable entity depending upon the activity or intervention. |
| **Irreversibility** | Irreversibility is the property of biometric templates which cannot be converted back into a raw image or probe. Most biometric templates unless Template Protected will not be irreversible. Reversible templates present privacy risk as unintended information about the subject will be present. This may enable an attacker to cause harm or distress to the subject. |
| **Legitimate Interest** | Legitimate Interest (LI) is one of several Lawful Bases in the General Data Protection Regulation. LI is a pathway which may be appropriate in circumstances where organisations choose to collect data based on business need, have no overriding legal requirement or other externality prompting collection, and are capable of assuming responsibility for the choice, with a corresponding obligation to make this choice in a balanced, structured way. |
| **Liveness Detection** | Liveness Detection is a feature which ensures that the subject presented to the system is in fact a live, present human. Liveness Detection may be unnecessary in 'manned' activity with an attendant, but vital if implementing remote or unattended biometrics, e.g. to prevent a subject from using a picture or image of another subject in order to bypass an authentication step. |
| **Pre-Processing** | Pre-Processing is a step undertaken within a biometric system before extracting features or producing a template. Pre-processing is often necessary for compensating for environmental or other conditions and if not undertaken correctly may result in high Failure rates at this stage of biometric events. |
| **Probe** | The term Probe in biometrics refers to the acquisition of data at one moment in time during a biometric event. For instance, when using a biometric passport kiosk a probe is undertaken to allow the kiosk to compare your face or hand with data held on your passport. |

| | |
|---|---|
| **Purpose Limitation** | Purpose Limitation is a principle in privacy which safeguards individual rights and freedoms by restricting the use of data to Purpose(s) identified prior to the collection of data, and which are specified to the individual. Use of data for an incompatible purpose is likely to be intrusive and unlawful. |
| **Renewability** | Renewability is a property of protected templates whereby they can be generated differently across multiple enrolment events with a subject. For instance, a system may store templates T1 and T2 on subject S which can both be used to identify the subject, but can be distinguished from each other such that if template T1 is stolen and subsequently used to authenticate it can be identified as NOT template T2 and therefore rejected - allowing in particular the prevention of fraud. |
| **Sensor** | A Sensor is a physical component used to capture data e.g. similar to a photograph, prior to the extraction from the data it produces into a template or other data used for biometric identification. |
| **Service Delivery** | Service Delivery is the term used throughout this document to refer to the fundamental intervention undertaken by an implementor and enabled by Biometrics - for instance a food distribution activity or cash and voucher transfer. |
| **Template** | The Template is the data structure produced by a biometric system and subsequently stored for comparison. It is a distillation of some characteristics or features from the raw data captured during a biometric probe, which is known or understood to be sufficient to re-identify the user later on using a biometric algorithm. |
| **(Biometric) Template Protection** | Template Protection, or BTP, is a family of techniques which add techniques to Templates which reduce certain privacy and security risks - in particular adding qualities such as Irreversibility, Unlinkability, and Renewability. BTP is described in ISO 24745 |
| **Threshold** | A Threshold is a value used to distinguish between and make decisions regarding specific biometric events. For instance, a biometric match below a threshold may be deemed by a system to be 'rejected' based on its dissimilarity with the template stored in the gallery, whilst a match above the threshold may be accepted. Thresholds may be configured for specific projects, areas, or across an entire system, and are one factor determining Accuracy. |
| **Tokenization** | Tokenisation is an approach to protecting data which substitutes a 'token' for the original record, reducing the number of places in which risky data is stored and allowing it to be protected more effectively. The token may be a random value or in some instances linked to or derived from the original data itself. Like all safeguards tokenisation addresses some but not all threat models. |
| **Transparency** | Transparency is a term from Data Protection which refers to the communication between an organisation and individual regarding how data is used. While there are specific requirements for Transparency in most data protection frameworks, it can be understood as similar and compatible with the principle of 'accountability (to affected populations)' in humanitarian practice - although the term Accountability itself carries a different meaning in data protection practice. |
| **Unlinkability** | Unlinkability is a property of some protected biometric templates whereby two templates produced by different systems from the same subject will not be possible to correlate with each other. This means that an attacker, for instance, who obtained biometric databases from Bank B and Government G, who both store data on subject S, would not be able to establish which records in B and G's databases belonged to S without additional data, offering significant privacy protection. In a field deployment this might, for instance, negate some risks whereby key populations could be exposed given a data breach. |
| **User** | Throughout this guidance the User is understood to be the human operating the biometric software or hardware. Other than where biometrics are remote and unattended the User is unlikely to be the Subject. The terms User and Attendant are generally used interchangeably in this guidance for this reason. |
| **Vendor** | A Vendor supplies some or all of a biometric system, but may provide specific components, services, or a combination. |
| **Verification** | See 1:1 |

## Appendix - Template for need/benefit analysis

| # | Requirement | Expected Benefit | Benefit for.. | Activity | Output | Outcome | Indicators | Notes & Purpose |
|---|---|---|---|---|---|---|---|---|
| EX | Donor Requirement - Use Biometrics to prevent fraud. | Reduction in 'double dipping' when goods are distributed. | Donor - effectiveness of spend.<br><br>Service Users - receive expected goods. | Biometric enrolment added to initial enrolment process; biometric verification added to distribution stage; staff appropriately trained; anti-corruption plan updated; community sensitisation plan drafted and rolled out. | Rollout plan + successful rollout based on criteria defined in the plan. | Program objectives are met - X distributed to Y people. | % of records with biometric GUID rises from 0% to 90% by Y.2<br><br>Reported instance of fraud drops from N per year to <=0.1N.<br><br>Recipients report a high level of satisfaction with a program - increase from N to 2N. | Purpose: Preventing Fraud.<br><br>We need to be sure to continue monitoring satisfaction levels and that false rejection does not increase.<br><br>We also need to ensure as we communicate, the intent of the program, and the intention to provide maximum distribution to communities needing assistance is well-communicated to contextualise the data collection. |
| EX | Use biometrics to de-duplicate data. | Link records together to allow better continuity of care. | Patient - records are available consistently across treatment sites allowing for better care.<br><br>Community - better measurement of vaccine rollouts, ensuring population-level protection. | Biometric enrolment added to initial enrolment process; biometric verification added during routine appointments; re-enrolment stage added for returning patients; staff trained; community sensitisation plan drafted and rolled out. | Rollout plan + successful rollout based on criteria defined in the plan. | Program objectives are met - care providers able to track patients across treatment sites leading to X health outcome. | % of records with biometric GUID rises from 0% to 95% by Y2.<br><br>Reported instance of mis-identification of health records drops from N per year to <=0.1N.<br><br>Patients report a high level of satisfaction with program - increase from N to 2N.<br><br>Care providers report Y health outcome. | Purpose: Providing healthcare to a high quality.<br><br>We need to keep track of disengagement from treatment to ensure it does not increase.<br><br>We need to continue re-assessing the health outcomes and clinical experience with clinicians to ensure our assumptions about engagement with treatment and continuity of care are correct. |

## Appendix - Biometric benefit analysis and maximisation

Aligning on the purpose, benefit, and activities can be complex with biometric technologies. The following tables, excerpted from the CovidAction-funded "Using Biometrics to fight Covid-19" paper provides a starting point which you may wish to use to begin your analysis:

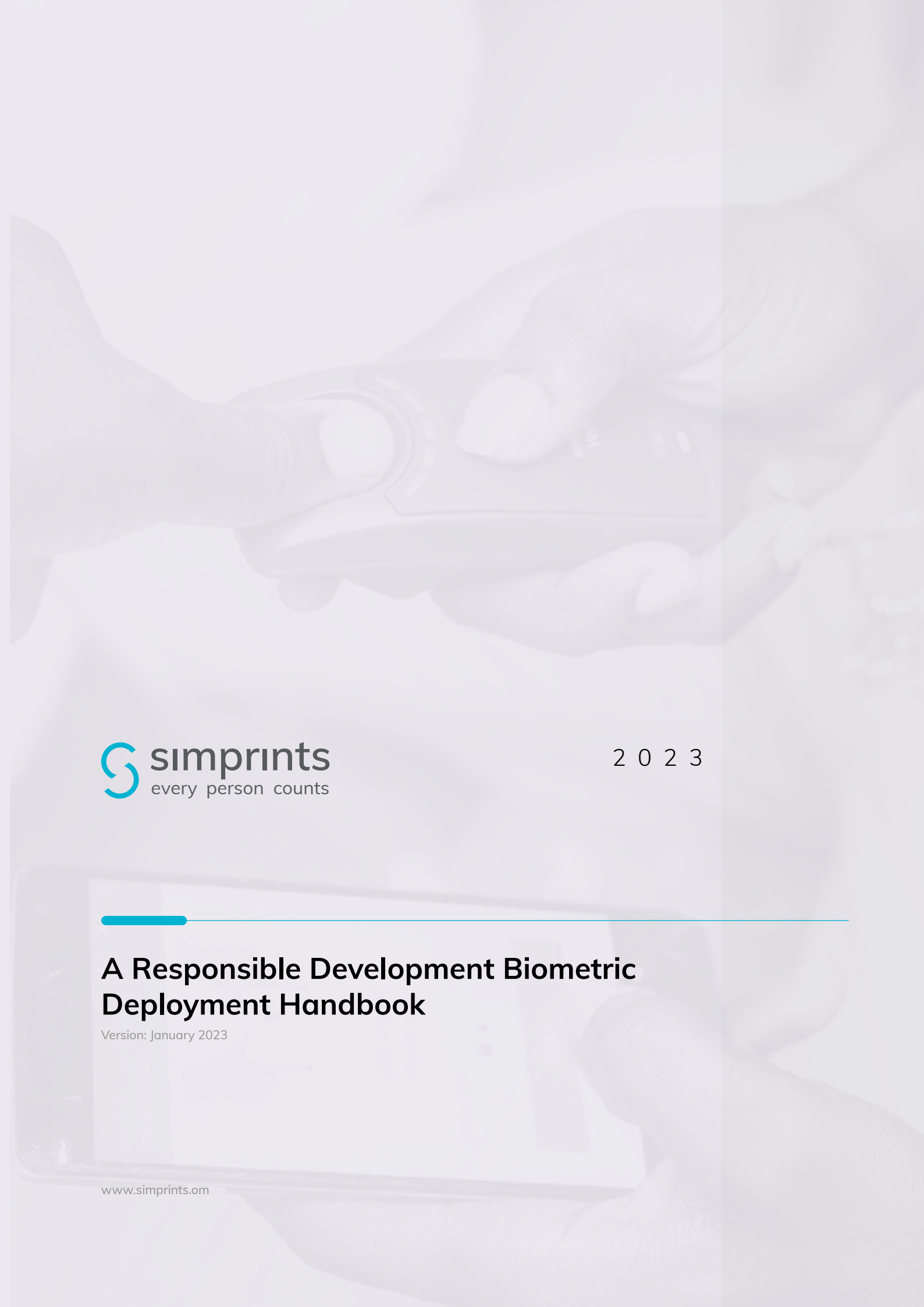
| Area of benefit | Benefit description | Primary benefit for whom | | | | | How to maximise this benefit |
|---|---|---|---|---|---|---|---|
| | | Patient | Health worker | Program Manager & M&E | Policy Maker | Funders & performance managers | |
| **User experience** | Ease retrieving records compared with a manual lookup using e.g. names or ID numbers | X | X | | | | Test and optimize workflow |
| | Improved continuity of care | X | | | | X | Ensure robust continuity of care practices are in place e.g. how to follow up after a missed appointment, how to treat a repeat attendee |
| **Data insights** | Verification of service delivery and collection of individual-level program data | | | X | | | Choose a biometric tool with high accuracy for the population the program is targeting |
| | Individual-level program data | | | X | X | X | |
| | Reduction in duplicate records | | | X | X | X | Export or visualise this data and implement processes to ensure effective use e.g in program decision-making |
| | No mixing between trial and control groups in clinical trials | | | X | | | |
| **Data privacy** | Reduced need for personal identifiers like names | X | | | | | Carry out effective community sensitisation to build trust |
| **Cost savings** | Reduction in wastage through better resource allocation (e.g. vaccines are delivered in the necessary quantities, and healthcare workers are mobilised to the correct locations). | | | X | | X | Implement continuous improvement practices |
| | Reduction in fraud | | | X | X | X | Implement automatic alerts of potentially fraudulent activity |
| **Efficiency** | Time saved when retrieving health records | X | X | X | | | Choose a biometric tool designed specifically for the setting, to prevent additional time wastage due to technology failures |
| | Reduction in additional M&E surveys/activities due to real-time data having already been collected | | | X | | | |

| | | | | | | | Risk Mitigation Strategy |
|---|---|---|---|---|---|---|---|
| | | Patient[55] | Health worker | Program Manager | Policy Maker | M&E teams | |
| **Infrastructure feasibility** | Technology ineffective due to lack of reliable connectivity[56] | X | X | X | X | X | Choose a biometric solution which works offline (with appropriate data security measures) |
| | Technology ineffective due to lack of reliable electricity[3] | X | X | X | X | X | Choose a wireless or portable tool, or factor power banks/generators into the project costs |
| | Technology ineffective in last-mile environment (heat, humidity, unpredictable light conditions)[3] | X | X | X | X | X | Choose a biometric tool designed specifically for the setting |
| **Technology challenges** | An individual cannot give biometrics (e.g. due to a lack of fingerprints) | X | X | | | | Implement a process when biometrics cannot be used to ensure access to services |
| | The algorithm fails to capture an individual's biometrics | X | X | | | | Choose a biometric tool with high accuracy for the population the program is targeting, and carry out system calibration. Implement a back-up process for when biometrics cannot be used to ensure access to services. Potentially include 2-factor authentication (a PIN or similar that is easy to remember to validate the match). |
| | An individual is misidentified | X | | | | | |
| **Rule of law and access to legal recourse** | Limited or non-existent privacy laws | X | | X | X | | Implement appropriate safeguarding within the project to protect patient privacy. Adhere to strict privacy regulations, even if not required by law. |

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

56 These risks apply to any deployment of technology and are not only limited to biometrics.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Patient rights, dignity, and informed consent** | People refuse to give their biometrics | | X | | | | Ensure people are informed of their rights in an easily-understandable way, and implement an alternative process when biometrics cannot be used to ensure access to services |
| | People are coerced into giving biometrics in order to receive services | X | | | | | |
| | People cannot access their rights due to illiteracy | X | X | | | | |
| | Personal data is used for purposes other than those originally intended | X | | | | | Assess all possible uses for biometric data before data collection begins, so that patients can be informed of their rights, and **find a way to update or later inform patients about new use cases.**<br><br>Conduct a Data Protection Impact Assessment<br><br>Separate biometric data from personal data when feasible so that misuse requires access to both to identify individuals. |
| **Data security** | Personal data is leaked, resulting in actual or perceived harm | X | | X | | | Choose appropriate data storage and database encryption options, and create a data security plan which must be followed in the case of a breach<br><br>Fund proactive monitoring of all biometric systems by IT security experts to be able to identify and respond to potential breaches. |
| **Other** | Locked in to one vendor due to a lack of interoperability | | | X | | X | Choose a biometric solution which offers interoperability with other systems and platforms. Use common standards for the biometric database and associated metadata. |
| | Community resistance to biometric data collection | | X | X | | | Carry out effective community sensitisation to build trust. Respect informed consent and not force anyone to use a biometric. |
| | The cost of back-up methods of identification may end up outweighing the incremental benefits of biometrics | | | X | X | | Carry out a cost/benefit analysis for the specific use case. Use an existing credential as a back-up method rather than implementing a new credential. |



simprints
every person counts

2023

# A Responsible Development Biometric Deployment Handbook

Version: January 2023

www.simprints.om