THE ROLE OF UNIQUE IDENTIFIERS IN CIVIL REGISTRATION & VITAL STATISTICS AND NATIONAL IDENTIFICATION SYSTEMS

August 2025



unicef
for every child

ESCAP
Economic and Social Commission for Asia and the Pacific

Get every one in the picture



*The shaded areas of the map indicate ESCAP members and associate members.**

The Economic and Social Commission for Asia and the Pacific (ESCAP) is the most inclusive intergovernmental platform in the Asia-Pacific region. The Commission promotes cooperation among its 53 member States and 9 associate members in pursuit of solutions to sustainable development challenges. ESCAP is one of the five regional commissions of the United Nations.

The ESCAP secretariat supports inclusive, resilient and sustainable development in the region by generating action-oriented knowledge, and by providing technical assistance and capacity-building services in support of national development objectives, regional agreements and the implementation of the 2030 Agenda for Sustainable Development.

**The designations employed and the presentation of material on this map do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.*

THE ROLE OF UNIQUE IDENTIFIERS IN CIVIL REGISTRATION & VITAL STATISTICS AND NATIONAL IDENTIFICATION SYSTEMS

August 2025

ISBN: 978-92-806-5690-9

© United Nations Children's Fund (UNICEF), Unicef Child Protection 2025

Cover image: ©UNFPA

unicef
for every child

ESCAP
Economic and Social Commission for Asia and the Pacific

Get every one in the picture

TABLE OF CONTENTS

1 ACKNOWLEDGEMENTS 1

2 SUMMARY 2

3 GLOSSARY 5

4 INTRODUCTION 8

5 KEY CONCEPTS 10

Legal identity 10

Foundational and functional registers 10

Legal identity management 12

6 UNIQUE IDENTIFIERS 13

Global and regional trends 13

Applications and benefits 15

Risks and concerns 18

Specific risks for people in vulnerable situations 21

Core principles for a good identifier 22

7 REFERENCES 26

1 ACKNOWLEDGEMENTS

This document was written by Nicola Richards (Consultant) under the guidance of Bhaskar Mishra (Child Protection Specialist – United Nations Child's Fund) and Tanja Sejersen (Statistician – Economic and Social Commission for Asia and the Pacific). It was reviewed by members of the United Nations Legal Identity Agenda (UNLIA) Task Force, and Members of the Asia Pacific CRVS Partnership, along with technical specialists including Julia De Bresser – International Organization for Migration; Martin Bratschi, Raj Mitra, and Romain Santon – Vital Strategies; Jeff Montgomery – Pacific Community; Sanjay Dharwadker, Conor Flavin, and Sam Jefferies – Office of the United Nations High Commissioner for Refugees; Emily Cercone – Independent Consultant; and Mia Harbitz – Global Financing Facility, World Bank Group.

The authors would like to acknowledge the substantial time and input provided by various organizations and individuals as part of an earlier draft of this guidance, initially developed in 2020, particularly UNICEF, UNDP Vanuatu, UNESCO, UN Statistics Division (DESA), World Health Organization Regional Office for South-East Asia, and Statistics Norway.

2 SUMMARY

Unique identifiers, often in the form of a unique identification number (UIN), are critical in the management of administrative records. They provide a unified means of identification across different systems and over time, facilitating both the statistical use of administrative data and improved service delivery for individuals, along with streamlining the administrative functions of government. They are generally the minimum requirement in the development and maintenance of administrative registers, given their ability to uniquely identify each unit in the register.

While the overall purpose of any system of identification is generally the same – to ensure the same individual can be repeatedly and correctly identified – the scope of unique identifiers as they relate to individual identification can range from narrow, facility-based applications that are program or sector specific, to national identifiers used across sectors, as follows:

- **National-level unique identifiers**, such as those found in foundational registers, create additional benefits beyond a single sector – with the ability, for example, to integrate data from health, social services, and education systems together to identify beneficiaries and provide holistic services.
- **Sector-specific identifiers** enable access to certain rights and services, such as healthcare. They are particularly beneficial when foundational registers do not have complete coverage of the population. In these instances, functional identifiers help to ensure all individuals who are eligible for a service can provide the necessary, sector-specific, credentials.
- **Facility-level identifiers** can help with improving the continuity of services provided to individuals, such as follow-up appointments in healthcare, or monitoring school absences; they can also improve the linkage of data over time and between facilities. They can improve the confidentiality of personal data by removing names and other personal identifiers from records.

Overall, benefits of unique identifiers include enabling reliable and efficient delivery of government services through improved identification and targeting of beneficiaries; strengthening linkages and preventing duplication between registers, thereby ensuring better control over data quality; reducing leakages in the distribution of welfare and social security benefits; and expanding the inclusivity of existing systems. Combining and consolidating information from multiple, separate systems or registries into a single register is both operationally efficient and cost-effective. Moreover, integrating data from multiple sources allows for cross-validation, further enhancing the accuracy and reliability of information.

Despite these advantages, the type of identifier and way it is used has a significant influence on both its utility and extent of data linkage it enables, as well as potential risks. Risks can arise during particular steps in the generation, assignment and use of unique identifiers. Other risks – including those relating to data protection and privacy, data security, scope creep, and the overall operating environment – while not directly due to unique identifiers, are often heightened when UINs are implemented.

- **Implementation level and scope**. When UINs are assigned nationally and used across many sectors, it increases the potential privacy risks associated with profiling and data linkage, particularly when data are saved in centralized databases, which introduces a single point of failure if data are ever stolen or hacked.
- **Data protection and privacy**. The extensive collection and storage of sensitive information about individuals that unique identifiers enable can create several risks to data protection and privacy including the potential to re-identify individuals, comprehensive profiling of individuals and population sub-groups by governments, and the creation of digital audit trails.
- **Data security**. Advances in the use of unique identifiers for a wide range of applications can pose a risk to the security of personal data, including the misuse of information by authorized users, and the unauthorized use of information – particularly when data are stored centrally.
- **Scope creep** refers to the disclosure and use of personal data for purposes not related to the original intent of data collection, and without the informed consent of individuals. The risk of scope creep is greatly enhanced by unique identifiers, given their ability to link data from various sources and systems.
- **Operating environment**. Concerns regarding the overall management and maintenance of the systems supporting the generation, assignment, and use of unique identifiers include the insecure or high-risk digital environments many electronic administrative systems operate in, and reliance on the private sector to provide telecommunications and financial infrastructure needed for the administration of electronic transfers, which can increase the risk of privacy and security breaches if not managed adequately.

Unique identifiers also pose specific risks for people in vulnerable situations and groups at risk of marginalization, including those relating to data protection and privacy, exclusion through system design or technology limitations and failures, and unintended uses of linked data. These individuals and groups are particularly vulnerable during the collection, analysis, and storage of their personal data, as they are often less aware of the risks and consequences of such processing, and of their rights and the safeguards in place to protect them.

In light of these benefits and risks, due consideration should be given to developing both robust identifiers and strong supporting systems. The characteristics of a good identifier depend partly on its intended use, for example, whether it will serve as a national unique identifier linking data across sectors, or as a sector-specific identifier with a more limited scope. In general, a good identifier should be unique, universal, and stable. The systems supporting the identifier should be inclusive, secure and privacy protective. Strategies for enhancing inclusion may involve accepting alternative forms of identification and ensuring that individuals without a UIN are supported to obtain one. Finally, systems should incorporate a comprehensive set of organizational, administrative, physical, and technical safeguards to ensure data protection and uphold privacy standards.

INTERESTED IN LEARNING MORE?

Practical approaches when planning for the use of unique identifiers (*currently in draft*) will provide practical guidance and tools to use when planning for the use of unique identifiers in administrative systems. It is divided into four sections:

1. **Initial planning and preparation**. Outlines several time-limited and one-off steps that should be conducted as part of initial planning and preparation. These steps lay the groundwork for successful implementation.
2. **Designing the unique identifier**. Provides an overview of technical aspects when developing an identifier. Key topics include assessing the characteristics that make a good identifier; exploring options for structuring the identifier; deciding on the number of digits required to ensure long-term sustainability; and addressing questions around the need for biometrics.
3. **Working towards implementation**. Describes the specific actions and broad conditions that should be in place as part of building and strengthening a supportive environment for the use of unique identifiers in administrative systems. Many of these relate to complex, ongoing activities that will require substantial resources and commitment from relevant stakeholders.
4. **Useful resources**. Includes a planning checklist and other practical tools to assist in the implementation process.


©UN Photo_Bernardino Soares

3 GLOSSARY

Term	Definition
Authentication	*See 'verification'.*
Civil registration	'The continuous, permanent, compulsory and universal recording of the occurrence and characteristics of vital events pertaining to the population, as provided through decree or regulation in accordance with the legal requirement in each country' (pp. 3) (1).
Data integration	The combination of technical and business processes used to combine data from different sources into a meaningful and valuable set of information. Data integration is an 'umbrella' term and can include combining data from multiple sources, combining geospatial data with other data, data pooling, record linkage, data fusion, and data prioritizing (when two or more sources contain the same data for the same variable) (2).
Data protection	Refers to the set of privacy-motivated laws, policies and procedures that aim to minimize intrusion into respondents' privacy caused by the collection, storage, and dissemination of personal data (3).
Data security	Refers to a set of physical, technological, and procedural measures that safeguard the confidentiality, integrity and availability of data and prevent its accidental or intentional, unlawful or otherwise unauthorized loss, destruction, alteration, acquisition, or disclosure (4).
Demographically identifiable data	Data points that enable the identification, classification, and tracking of individuals, groups, or multiple groups of individuals by demographically defining factors. These may include ethnicity, sex, age, occupation, and religion (4).
Digital identity	'… a collection of electronically captured and stored identity attributes that uniquely describe a person within a given context and are used for electronic transactions… A person's digital identity may be composed of a variety of attributes, including biographic data (e.g., name, age, gender, address) and biometric data (e.g., fingerprints, iris scans) as well as other attributes that are more broadly related to what the person does or something someone else knows about the individual…' The attributes and authentication factors used in a digital identity may vary from one context or country to the next depending on the type of identity system' (pp. 11) (5).
Foundational identity registers	Foundational identity registers include civil registries, national identification and population registers. They are created to serve as authoritative sources of legal identity information for the general population and to provide proof of identity for a variety of public and private sector use cases (6).

Term	Definition
Functional registers	Functional registers are created to manage identification, authentication and authorization for a particular service or transaction, such as voting, tax, social programs and transfers, or financial services. Functional identity credentials—such as voter IDs, health and insurance records, tax ID numbers, ration cards, driver's licenses, etc.—may be commonly accepted as proof of identity for broader purposes outside of their original intent, particularly when there is no foundational ID system (6).
Legal identity	'The basic characteristics of an individual's identity, e.g., name, sex, place and date of birth, conferred through registration and the issuance of a certificate by an authorized civil registration authority following the occurrence of birth. In the absence of birth registration, legal identity may be conferred by a legally recognized identification authority; this system should be linked to the civil registration system to ensure a holistic approach to legal identity from birth to death. Legal identity is retired by the issuance of a death certificate by the civil registration authority upon registration of death' (pp. 9) (7).
Legal identity management	'The term refers to the issuance of a proof or legal identity to each individual by a government-authorized entity and the maintenance of systems for managing information and documents associated with such identity. It also comprises verification, registration, management, and conservation of personal data of citizens as well as non-citizens on the state territory, with the goal of establishing unique legal identity credentials within the jurisdiction. Identity management usually includes all data from the civil registration of a person and may include other attributes such as a unique number and/or biometric data, including identification credentials issued by an identity management agency that serve as a basis for the verification of identity (i.e., passport or national identification cards)' (pp. 11) (7).
Personally identifiable information (PII)	Refers to data and information related to an individual who can be identified from that data; from that data and other information; or by means reasonably likely to occur through use of the data. PII includes biographical data such as name, sex, name of parents, marital status, date and place of birth, country of origin, individual registration number, religion and ethnicity, biometric data such as a photograph, fingerprint, facial or iris image, as well as any expression of opinion about the individual, such as assessments of the status and/or specific needs (8).
Population register	A database of every individual that has the right to reside in the country, including citizens and non-citizens, children and adults. Population registers typically contain demographic data and life-event information that is the basis of or exchanged with other identification systems and databases such as national identification systems, civil registers, and others (6).
Privacy	'The right and ability of an individual to control the extent, timing, and circumstances of sharing themselves (physically, behaviorally, or intellectually) with others. This includes limiting access by others to aspects of their person that can include their thoughts and identifying information' (pp. 19) (9). Data privacy, for example, refers to the freedom from intrusion into one's personal information (2).

Term	Definition
Record linkage	'Record linkage refers to the identification and combination of records corresponding to the same entities – for example, persons, enterprises, dwellings and households – throughout two or more data sources. Record linkage methods can be classified into two branches: deterministic… and probabilistic matching' (pp. 35) (2). *Also referred to as 'data linkage'.*
Unique health identifier (UHI)	'A UHI is defined as the designation permanently assigned to an individual for identification and should be governed by an independent central trusted authority. A UHI consists of a unique sequence of numbers and characters which provide a lifelong unique identifier for an individual and must support positive identification of an individual, automated linkage of electronic records, streamlining of records management and provision of a mechanism to strengthen security' (pg. 1) (10).
Unique identification code (UIC)	*See 'unique identification number' (UIN).*
Unique identification number (UIN)	'A number that uniquely identifies an individual and can be used to link an identity across databases and systems in both the public and private sector. National identity providers may issue a UIN to citizens and residents for their lifetime' (pp. 8) (5).
Verification	The process of verifying an individuals' claimed identity against registered identity information; in other words, the process by which a person proves that they are who they say they are. Once a person has been registered and credentialed, they can use their identity to access benefits and services to which they are entitled (1).

4 INTRODUCTION

Unique identifiers, defined simply as '… sequences of characters that identify an entity' (11), are critical in the management of administrative records, including those found in civil registration and vital statistics (CRVS) and identification systems. Identifiers are generally issued when an individual enrolls into a system and serve as a record locater or index within the system to facilitate processes such as linking records within a database (6). They are increasingly important in identity management and data linkage – both within and between line ministries, and among the private sector. Identifiers may apply in foundational and functional administrative registers and can take a broad range of formats; they may be unique to a specific 'site' (such as a hospital or school), a single sector (such as health or education), or applied across different sites, sectors and systems.

The ability of individuals to prove their identity – and the ability of governments to accurately identify beneficiaries – is a direct or indirect enabler of several Sustainable Development Goals, including those relating to gender equality and empowerment, access to basic health and education services, and child protection (7). In health, which has the most extensive history with unique identifiers, identification is crucial for the efficient and effective delivery of health care services and public health management, with providers needing to access correct medical and treatment histories to ensure consistent and appropriate care is provided; patients needing documentation to prove their enrolment in programs and safety nets to cover expenses; and administrators and researchers needing unique identifiers to de-identify and aggregate records and share data for statistics, planning, monitoring, evaluation, and research (12). In civil registration and identification systems, unique identifiers provide a unified means of identification between agencies and over time – facilitating both improved service delivery, along with streamlining the administrative functions of government.

Despite their advantages, the type of identifier and the way it is used have a significant influence on its utility, the possibility of data linkage it enables, and on potential risks. Risks can arise at specific stages in the generation, assignment and use of unique identifiers, while other risks are cross-cutting – including those relating to the implementation level and scope of the identifier, data protection and privacy, data security, scope creep, and the overall operating environment (13). Unique identifiers also introduce specific risks for people in vulnerable situations and groups at risk of marginalization. These risks encompass issues such as data protection and privacy, exclusion through system design or technology limitations and failures, and unintended use of linked data. As with any system that collects, analyzes, and uses personal data, balancing the benefits and potential risks of unique identifiers is complex and requires careful consideration. Addressing these challenges demands special attention to ensure that the systems are equitable, secure, and respectful of individual rights.

Despite their growing importance and widespread use, there remains limited specific international standards that regulate or contain recommendations on the assignment of unique identifiers. As such, the aim of this document is to obtain a better understanding of the various approaches to unique

identifiers being used in administrative systems, common and emerging practices globally, current international recommendations (and their consistency across sectors), and the benefits and risks of these approaches – with the goal of providing deeper understanding on how unique identifiers can be applied to CRVS and identification systems.

This document primarily addresses the needs of government officials working in national civil registration and/or identification systems, and their key partners. While the specific stakeholders may vary by country, it will generally involve a combination of staff from the civil registration office (Ministry of Justice, Interior, or Home Affairs), staff from the identification agency, ministry or department (if separate from civil registration), staff from the policy and planning or health information unit of the Ministry of Health, staff from the National Statistics Office, and other relevant government agencies.



©UNFPA

5
KEY CONCEPTS

Legal identity

The ability to be identified and formally recognized as a person before the law is the foundation that underpins the recognition and realization of human rights and is an essential tool for effective participation in modern society (6, 7). The inability to prove a legal identity when interacting with the state and private organizations is a major barrier to accessing many basic human rights and services, including education, healthcare, and social/financial transfers (14). The right to a legal identity for children, starting at birth through civil registration, is enshrined in both the Universal Declaration of Human Rights and the Convention on the Rights of the Child (CRC); and is recognized as a key development goal under the 2030 Agenda for Sustainable Development, Target 16.9: 'Legal identity for all, including birth registration, by 2030' (7).

Through recording vital events such as births and deaths, an effective civil registration system provides the official record of the existence of a person and recognition of that individual before the law, and is a fundamental means of granting legal identity, defined as:

> '… the basic characteristics of an individual's identity, e.g., name, sex, place, and date of birth conferred through registration and the issuance of a certificate by an authorized civil registration authority following the occurrence of birth. In the absence of birth registration, legal identity may be conferred by a legally recognized identification authority; this system should be linked to the civil registration system to ensure a holistic approach to legal identity from birth to death. Legal identity is retired by the issuance of a death certificate by the civil registration authority upon registration of death' (pp. 7) (6).

Foundational and functional registers

Registers are systematic, structured lists of 'units' (individuals, organizations, businesses, etc.), which contain identifiable unit-level data on each unit (such as the personal details of an individual) and usually have some sort of regular updating mechanism that allows established datasets to be updated, corrected, extended, or retired (15). Registers can be broadly grouped into (16):

- **Administrative**: primarily used for public administrative purposes in a government management information system. Apart from civil registration and vital statistics systems, other examples include tax registers to record information on income, property and other taxes; education registers to record student information; and medical registers to record health information.
- **Non-administrative**: operated by private organizations for business purposes, fulfilling non-public administrative needs. A register of incorporated societies, for example, includes information on the names, addresses and dates of membership of a society's members.

- **Statistical**: created by processing data from administrative and non-administrative registers for statistical purposes. Statistical registers may act as data coordination tools, integrating data from several sources through linkage.

Foundational identity registers provide 'general purpose' identity as a public good for use across sectors – they are typically owned and operated by the government, are mandated by thorough legal frameworks, and aim for full population coverage and completeness (14); provide credentials that can function as an official form of identification, i.e., legal identity; and can underlie multiple sector-specific, functional purposes (6). The registration of births through civil registration is the starting point for establishing an individual's legal identity. It also provides the foundation for enrolment in the civil register, identity management systems, and other administrative registers (17), including population registers (see **Box 1**).

Functional registers, in contrast, serve a specific function (such as the delivery of healthcare services, or voter eligibility for an election); they may or may not be linked to other systems supporting other functions; often only cover a subset of the total population (with many functional registers excluding children and non-nationals); and any given person may have a variety of functional identities (6). When different government agencies or ministries, private companies, non-governmental organizations (NGOs), aid agencies, etc., create their own functional systems to support their work, this narrow focus on institutional goals can lead to siloed sectoral systems, where one person has different identifiers for health insurance, education, and social benefits, for example (18).

BOX 1

WHAT ARE POPULATION REGISTERS?

Population registers are an inventory of all residents in a geographic area (usually a country) that contain current information on vital events from the civil register, and other information, including residential address. Population registers are usually built from an existing inventory of information (such as a census, existing civil or identity register, or mass enrolment campaign), and, through the linking of individual records across different administrative registers and databases, can be updated.

Two important principles of population registers are that each person only gets one record in the register, and personal information is registered once and used for multiple purposes. The primary role of population registers in identity management is to act as the major reference point where other functional registers can check the legal identity of individuals, generally through cross-checking their unique identification number.

For more information see:

ESCAP Stats Brief – Population Registers: A key resource for producing vital statistics (October 2020)

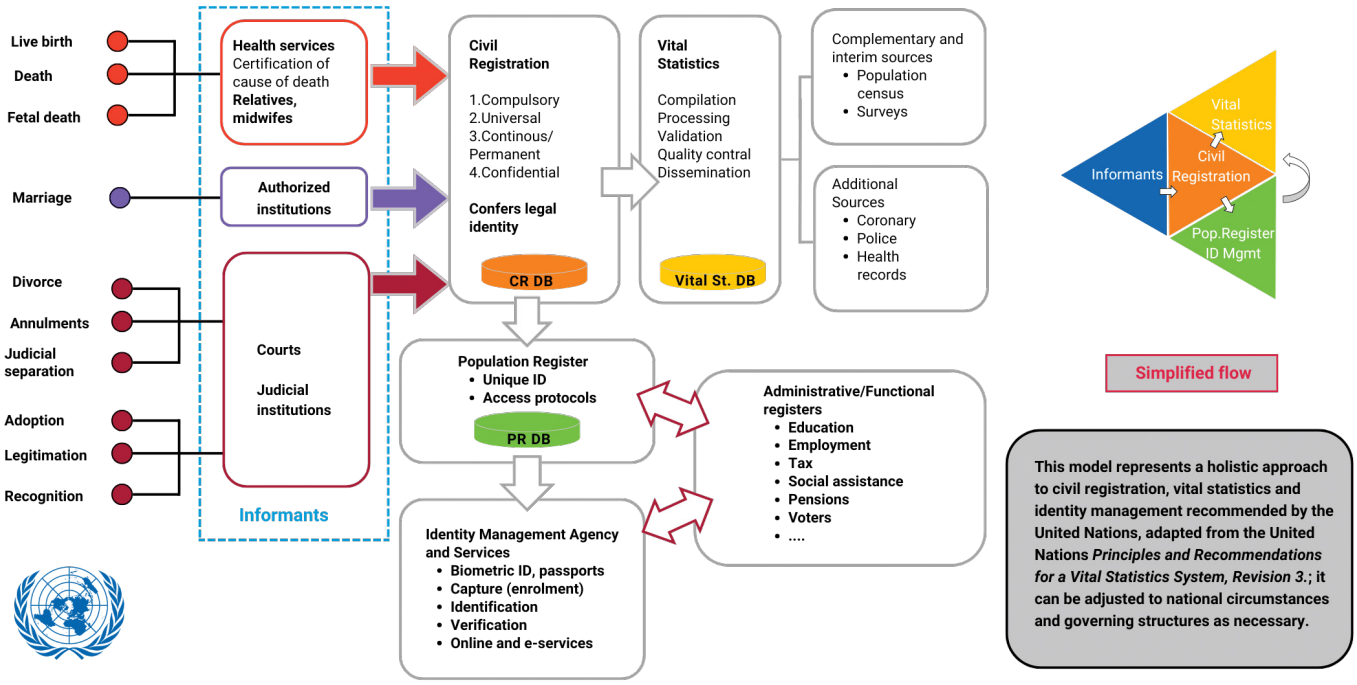
Available here

Legal identity management

Holistic legal identity management requires strong civil registration and identification systems that may be linked directly or linked through population registers (17), as demonstrated in **Figure 1**. While there is no internationally agreed definition of legal identity management, the term refers to the issuance of proof of legal identity to each individual by a government-authorized entity and the maintenance of systems for managing information and documents associated with such identities (7). It comprises the verification, registration, management, and protection of personal data, with the goal of establishing unique legal identity 'credentials' (such as unique identification numbers, identity cards, official certificates, etc.) (1, 19). Identity management systems usually combine data from the civil registration of a person with other attributes such as biometric data, along with identification credentials issued by an identity management agency that serve as a basis for verification of identity – such as unique identifiers and national identification cards (7).

A country's legal identification system can provide a supporting framework for observing and protecting many of the rights embodied in international declarations and conventions, ensuring that residents can exercise their rights and access services and benefits, with secure identity management seen as the foundation for other branches of state services and functions (19). Inclusive and trusted national identification systems can help to strengthen the transparency, efficiency, and effectiveness of governance and service delivery by enhancing the ability of departments and agencies to identify and include beneficiaries in their systems and reduce common challenges such as fraud (6). Flawed identification systems, conversely, can disrupt the effectiveness of government activities, and may exclude individuals or specific groups of the population from accessing services and benefits perpetuating inequality and marginalization (19).

Figure 1: Civil registration, vital statistics and identity management systems



Key: CR DB – Civil registration database; Vital St. DB – Vital statistics database; PR DB – Population register database

Source: United Nations Statistics Division. Guidelines on the legislative framework for civil registration, vital statistics and identity management systems New York: UNSD, Department of Economic and Social Affairs, Statistics Division; 2023.

6 UNIQUE IDENTIFIERS

Recent decades have seen changes in the volume, velocity, and variety of personal data stored, creating a shift in how personal information and other data are processed and stored, and increasing the need for a variety of techniques for individual identification using unique identifiers (19, 20). A unique identifier, often in the form of a unique identification number (UIN),[1] is a sequence of numbers, letters, or characters assigned to an individual[2] for the purpose of uniquely identifying that individual to enable their identification across systems (3, 21). Identifiers are considered 'unique' when the number-generating process ensures that no two people within the system have the same number, and if needed, a de-duplication process ensures that the same person does not have multiple identity records or numbers in the database (6).

Unique identifiers are relevant in all administrative systems, including civil registration and identification, as they provide a unified means of identification across different systems and over time – facilitating both the statistical use of administrative data and improved service delivery for individuals (22), along with streamlining the administrative functions of government (14). They are generally the minimum requirement in the development and maintenance of administrative registers, given their ability to uniquely identify each unit in the register (22), and as such, play a critical role in linking the national data infrastructure (23). While identification is possible without unique identifiers by using sufficient biographic and demographic information (such as name, sex, date of birth, address, etc.), this approach is not practical on a large scale, there is the risk that some information may be mistyped, and different people may have identical personal information (18, 19, 24). Unique identifiers can also be used for verification in both foundational and functional registers – serving a similar function as a unique username to say, 'this is who I am' (6).

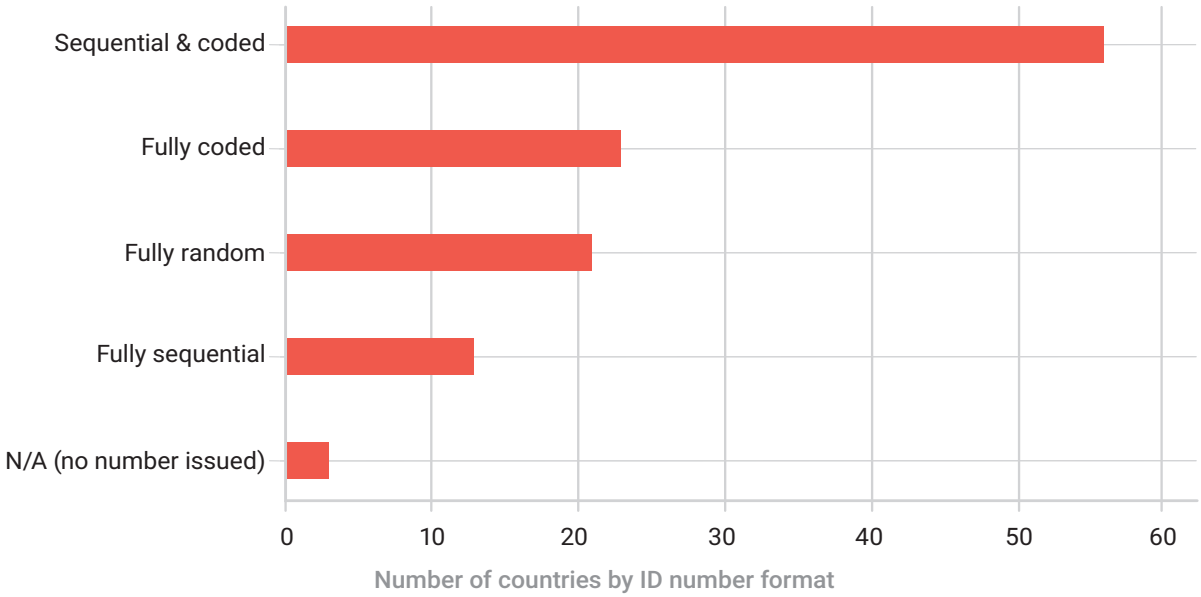
Global and regional trends

According to the recent Identification for Development (ID4D) Dataset (25), as of mid-2022, 175 countries had some form of foundational system, such as a national identity, population register, or similar system, which issues general-purpose (foundational) identification for adults. Of the countries that provided further information, 96% of ID numbers issued by the system were permanent, 71% of ID numbers were assigned at birth, and 57% of ID numbers were recorded on the birth certificate. The ID numbers ranged in length from seven to 20 digits, but most were around 10–13 digits. Only 21 countries reported generating completely random ID numbers (**Figure 2**). The most common ID number format was a mix of coded and sequential digits. Common information coded into ID numbers included date of birth (49+ countries) and sex or gender (42+ countries). In addition to biographic data, most foundational identity systems (at least 152) also collected biometrics – most commonly fingerprints and facial images.

1 Also referred to as a 'unique identification code' (UIC) and 'personal identification number' (PIN). For simplicity, 'unique identification number' (UIN) is used in this document – refer to the glossary for more information.

2 Technically, unique identifiers can be used to identify any 'unit' – including individuals, organizations, specific facilities, etc. For this document, individuals are the defined unit of interest.

Figure 2: Frequency of ID number formats (from 116 countries surveyed)



Adapted from: Casher C, Metz A and Clark J. ID4D Global Dataset Volume 3: Trends in Identification for Development. Washington, DC: World Bank; 2024.

There is an increasing preference for random identifiers over coded or structured identifiers. Random identifiers provide a higher level of security by making it difficult to reconstruct or guess the identifier, thereby reducing the risk of unauthorized access and protecting personal information. The 12-digit Individual Identification Number (IIN) introduced in Kazakhstan in 2008, for example, which included data on date of birth and sex, was replaced in 2024 with a totally randomised number. Türkiye's 11-digit Identity Number, implemented in 2000 as part of broader a digitalisation project, is totally randomized.

Based on regional surveys on identity management practices, at least 93 countries assign a UIN at some stage in the life cycle of its citizens and/or residents – primarily in Europe and Central Asia (where 66% of countries in the region have a UIN), followed by South Asia (38%), and East Asia and the Pacific (35%) (17, 18, 26). Of the countries sampled by the World Bank in 2016 that included digits or characters indicating personal information in their identifiers, the most common characteristic included was date of birth (75%), followed by location (43%), sex (32%), and nationality/citizenship (18%) (noting that many coded identifiers contain multiple characteristics).

Similar results were highlighted in a 2017 review of identity management practices in the European Region (19), with the Organization for Security and Co-operation in Europe finding that 82% of countries in the region used coded identifiers and 76% used the same UIN across government services. A further review of legal identity management systems organized by the UN Economic and Social Commission for Asia and the Pacific (ESCAP) in 2021 (26), found that of the 26 countries who have mandatory national ID programs, 23 also had a system of unique identifiers, while one country was in the process of implementation.

Applications and benefits

While the overall purpose of any system of identification is generally the same – to ensure the same individual can be repeatedly and correctly identified – the scope of unique identifiers as they relate to individual identification can range from narrow, facility-based applications that are program or sector specific, to national identifiers used across sectors (19, 27). As the scope of identifiers is expanded, so too does the complexity of the systems required to support the generation, assignment and use of unique identifiers (28). Benefits and risks also increase as the scope and use of identifiers are expanded. Countries such as Denmark, Finland, Iceland, Norway, and Sweden, who were the first in the world to introduce national unique identifiers, are characterized by their broad scope, with national UINs used across almost every administrative sector and register, as well as the private sector for banking, mobile phone ownership, and the management of household utilities (10). More recently, similar systems of unique identifiers have been implemented in a diverse range of countries, including Botswana, Chile, India, Malaysia, Singapore, South Africa and Thailand.

Conversely, countries such as New Zealand have taken a particularly strong position to limit the use of 'ubiquitous'[3] foundational identifiers, with the Privacy Act of 2020 explicitly stating that, an agency '…may not assign to an individual a unique identifier that, to [the agency's] knowledge, is the same unique identifier as has been assigned to that individual by another agency…' (29). Similarly in Australia, the *Guidelines to the Information Privacy Principles* written by the Office of the Victorian Information Commissioner, have included a clause to; '… prevent the creation of a single identifier that could be used to cross match data across all Government Departments' (pp. 3) (30).

Broadly speaking, unique identifiers can be used for two main reasons: the management of administrative registers that store individuals' data for the purpose of service delivery and identity management (*the focus of this document*), and for statistical, research, and policy needs (via data linkage). As the two applications are conceptually very different, unique identifiers used for statistical, research, and policy needs generally cannot be 'retrofitted' for use in identity management (31).

Individual and/or administrative management

Most government agencies are looking for opportunities to better coordinate program delivery, with discrete administrative data collections often leading to a fragmented and incomplete picture of an individual's overall service utilization within and between sectors (31). When designed properly not to contain any identifying information, UINs can also enhance confidentiality – allowing individuals to access services without having to provide their name or other personal information (32).

Foundational, national unique identifiers

National (also referred to as ubiquitous or global) unique identifiers, such as those found in foundational civil or identification registers, create additional benefits beyond a single sector – with the ability, for example, to integrate data from health, social services, and education systems together to identify eligible beneficiaries and provide support services (17, 33, 34). Benefits include the accurate and efficient delivery of government services by being better enabled to identify and target beneficiaries,

3 The term ubiquitous refers to something that is existing or being everywhere at the same time, or very widespread. A ubiquitous unique identifier is one that is used across all services, systems, transactions, etc.

increasing linkages and avoiding duplication between registers, offering more reliable control over the quality of the registers' content, reducing leakages in the distribution of welfare and social security benefits, and increasing the inclusivity of existing systems by streamlining authentication processes (3, 22, 35). The combination and consolidation of information from multiple and separate systems or registries into a single register is both more efficient and cost-effective from an organizational perspective – while the integration of data from multiple sources helps to validate the data collected from one source (23, 36).

The wider range of benefits from national unique identifiers also includes (10, 28, 23, 37):

- reducing the burden on individuals to demonstrate their identity credentials,
- avoiding duplication of effort for individuals and organizations,
- the ability to accurately de-duplicate repeated elements of information and streamline record management,
- the ability to develop a comprehensive, longitudinal record of a person's service use that might not be otherwise available from a single source or occasion of service,
- strengthened systems for person-centered monitoring and improved linkage between services,
- the ability to access and integrate information from different service providers and different electronic information systems,
- the ability to assess and improve data quality throughout the system, including reducing the likelihood of contradictory identity credentials/records and preventing identity theft, and
- improving the management of programs and services.

The national ID number of Thailand, for example, is generated by the Bureau of Registration Administration under the Ministry of Interior during birth registration and is stored in the population register. The number is used to register children for school, apply for a driver's license, and to request other identity-related documents. Since 2001, the number has been used to identify citizens and eligible residents for the delivery of healthcare as part of Thailand's Universal Coverage Scheme (38). In Estonia, citizens are registered at birth in the population register and issued with their unique personal identification code (PIC). The population register is updated daily on vital events (births, deaths, marriages, etc.) and the databases of over 900 organizations can share information, including the health sector. Newborns are entered into the population register through birth registration and are linked to their mothers' PIC and/or electronic identity (eID) and automatically entered as beneficiaries in the country's universal healthcare scheme, guaranteeing them access to healthcare services from birth (12).

Functional, sectoral identifiers

Sector-specific identifiers enable access to certain rights and services, such as education, healthcare, social protection and voting. They are particularly beneficial when foundational registers do not have complete coverage of the population (such as low rates of birth registration, or national ID cards that are only available to adults). In these instances, functional identifiers help to ensure all individuals who are eligible for a service can provide the necessary, sector-specific, credentials (12).

When using unique identifiers for the management of individuals within a specific sector, the primary aim is to identify all the records associated with an individual and to examine or analyze some aspect (or aspects) of their data for purposes relating to the provision of a service to that individual (31). In the education sector, for example, identifiers are used to ensure that a child's education data move with them as they progress through grades, and as they move between different educational facilities – such as the Scottish Candidate Number (SCN) assigned to all pupils in primary and secondary schools. This allows for linkage of education datasets including those relating to the Annual School Pupil Census; attainment data from the Scottish Qualifications Authority; Attendance and Absence and Exclusions Surveys; and the National Statistics School Leaver Destinations Survey (39–41).

As different sectors need different kinds of data, the ability to segregate identity data into sector-specific segments and cater for discrete management policies by sector and data type is gaining increased attention. This has particularly been the case in healthcare, where the risks of re-identifying individuals from their national identification number may negatively impact patient privacy (42). The use of UINs in healthcare helps to ensure that each patient has one unique identity within the health system, facilitating the development of longitudinal medical records. This improves access to – and the integration of – information from different providers and provider systems, while supporting population-based medical research and development (32, 43). In enabling connections across fragmented data systems, UINs can help ensure that accurate information is attached to the right patient – helping to reduce the risk of medical errors, inappropriate care, loss to follow-up and redundant tests (10, 12, 20, 27).

Functional, facility identifiers

In certain settings, often those with paper-based records or highly decentralized systems, each facility may create their own identifier, which may or may not be linked with other identifiers in the country (28). Though the utility of such identifiers is limited, facility-level identifiers can help with improving the continuity of services provided to individuals, such as follow-up appointments in healthcare, or monitoring school absences; they can also improve the linkage of data over time and between facilities. They can improve the confidentiality of personal data by removing names and other personal identifiers from records (28).

De-identified statistical linkage

Unique identifiers enable more efficient statistical data linkage – the process of combining records about the same individual from two or more different data sources to produce interesting, novel, accurate, and valuable knowledge, with the aim of providing better information to inform public policy, generate statistics, and enable research (31, 36, 44). There are two main methods in statistical data linkage: deterministic, which generally requires a unique identifier for exact linkage; and probabilistic, which takes into account the different discriminatory powers of various attributes or characteristics of an individual (their name, date of birth, sex, etc.,) to calculate an overall score on the probability that two records belong to the same individual (36, 45).

Statistical linkage can help an agency better understand the patterns of service use by groups of clients (such as women and girls, or internally displaced persons), and in doing so, identify gaps or overlap in service provision between programs or across agencies, as well as the progression pathway of client groups through a service (31). Linking records from health and non-health sources, for example, is popular in countries such as Australia, Bhutan, Brazil, Canada, the United Kingdom, and United States of America – contributing significantly to the advancement of knowledge, health services research, changes in clinical practice, health policy reforms, and policies to reduce poverty and social inequalities (36).

Linkage for statistical purposes is generally done over a shorter timeframe (usually the study period, with records and databases destroyed at the end), has a lower cost, and has different privacy and confidentiality issues than linkage for client or administrative management (31, 46). Importantly, with statistical linkage, a small degree of error is acceptable, and beyond saying 'record A belongs to person A', the identity of an individual is not important, with data generally always de-identified (32). Most statistical agencies, for example, follow the 'separation principle' – in that identifying information is not included in the linked data for statistical analyses (37).

Risks and concerns

All identity management systems require data about individuals to be collected, analyzed, and stored, and this can raise significant risks and concerns over the vulnerability of the approach in terms of the protection and use of individuals' personal information (7). Risks can arise during particular steps in the generation and assignment of unique identifiers, particularly when data are transmitted within and between facilities, agencies, and sectors. Other risks cut across all elements of any system using UINs – including those relating to data protection and privacy, data security, and the overall operating environment (13). While not inherently a risk of unique identifiers, these risks are often heightened when UINs are used (as shown in **Table 1** using the example of healthcare).

Table 1: Pros and cons of the different methods for generating a national unique health identifier (UHI)

Method of assignment	Benefits	Risks/challenges
National UIN is used as UHI	Can connect with other systems beyond the health sector Lower costs associated with infrastructure and human resources Multiple identities cannot be issued for the same person within the health sector	Consequences of data breaches are likely to be more serious than for sector/facility identifiers Not all health service users may have a UIN or have proof of their UIN
National UIN and UHI are both used and linked to each other	Potential to connect with other systems beyond the health sector Lower risk of misuse of the national UIN by having a separate UHI	Higher cost of maintaining the infrastructure and human resources required for two identity management systems Potential for misuse of sensitive health data
UHI is assigned, not linked with national UIN	Increased confidentiality given the limited scope and use of the UHI (to the health sector only)	May further a fragmented and siloed approach to service delivery and data at the sector level Likely to create challenges for national identity management systems, including contradictory identity credentials between systems Higher cost of maintaining the infrastructure and human resources required

Key: UIN = unique identification number; UHI = unique health identifier

Adapted from: Mills S, Lee JK, Rassekh BM, et al. Unique health identifiers for universal health coverage. Journal of Health, Population and Nutrition. 2019: 18; 38 (Suppl 1): 22.

Implementation level and scope

When UINs are assigned nationally and used across many sectors, it increases the potential privacy risks associated with profiling and data linkage, particularly when data are saved in centralized databases, which introduce a single point of failure if data are ever stolen or hacked (30, 32, 35). The Unique Identification Authority of India (UIDAI), for instance, has implemented stringent security measures to protect the country's 12-digit unique identification number (Aadhaar). Despite this, there have been several instances of data breaches, with the most recent involving the leakage of uniquely identifiable information (Aadhaar and passport numbers) of 815 million people on the dark web (47). The concept of national identifiers can also be met with strong resistance from the general population, as demonstrated in several countries where significant political concern and scrutiny led to the reversal and ultimate end of proposed national ID schemes (34, 35).

Conversely, the use of several functional identifiers can generate a fragmented approach to identity management, with overlapping and incompatible systems producing multiple identities for the same individual distributed across several government organizations (14, 33). Sectoral identifiers can be costly, with the potential to over-design systems to meet more specific (and limited) needs also limiting the possibility of responsibly reusing technical systems (12). The expertise needed to establish and maintain the registers supporting the UINs may not exist in a very fragmented system, particularly when implemented at the local level. Further, while issuing identifiers manually at the facility-level is often easier in the short-term, it can create longer-term issues. Medical record numbers, for example, are generally issued and maintained by individual facilities, with the numbering system specific to each clinic or hospital. As such, they are not truly 'unique' identifiers as one person may have many, and the same number may be used across facilities for different people (32).

Data protection and privacy

The extensive collection and storage of sensitive information about individuals that unique identifiers enable can create several risks to data protection and privacy, including (34, 35):

- **The potential to re-identify individuals**. Identifiers that are based on personal characteristics (such as date of birth, sex, location, etc.) can be used to isolate information about an individual for profiling and/or identity abuse and theft. Re-identification is a particular concern when dealing with 'small cell data', for example, a rural health facility where it would be relatively easy to re-identify patients based on personal data contained in their UIN. Serial numbers can also provide a sense of when enrolment in a system occurred, with higher numbers indicating more recent enrolment.

- **Comprehensive profiling of individuals and population sub-groups by governments**. UINs enable the linking of disparate information across databases and this linkage deepens insight into individuals and population subgroups (for instance, refugees or ethnic minorities), with the sum of all the data more invasive than its individual parts (14). This risk is particularly high when a single national identifier is used across many sectors and systems, and when data are centralized, which in itself increases the risk of unauthorized access (7, 48).

- **The potential for overbroad and unnecessary data access.** Unless systems implement sophisticated and stringent access controls (including access provision, review, and revocation), UINs can increase the risk of unnecessary data access, violating individual privacy. This risk of unnecessary data access is increased when there are weak and inadequate retention and destruction policies

and procedures, particularly for 'multi-purpose' databases that may contain a variety of personal information. In such instances, there is the risk that all data will be kept personally identifiable for longer than necessary, running counter to data protection requirements and with implications for data accuracy and security.

- **The creation of digital audit trails**. Unique identifiers help to facilitate the creation of mega-sized databases that may contain UINs, biometrics, personal directory data, locational data, device identifiers, transaction details, and other personally-identifiable information that is not the direct outcome of a controlled environment for the collection and storage of data, but the by-product of identity-facilitated use (14). Such databases can create significant concerns over data security, exploitation, and misuse. They also have the potential for harm by further solidifying existing exclusions and increasing the potential for malevolent individual surveillance, profiling and privacy abuse, with initially 'benign' systems later used for other purposes (7, 34).

Data security

Advances in the use of unique identifiers for a wide range of applications can pose a risk to the security of personal data, including the misuse of information by authorized users, and the unauthorized use of information (18, 32). Such breaches in data security can reduce trust, undermine individual rights to privacy and consent, and put vulnerable groups at risk of harm (12). The centralization of data, for example, while essential for foundational databases to ensure the de-duplication of identities/identifiers, increases privacy and security threats (14), with the existence of large repositories of sensitive information on entire populations increasing the risk of deliberate attacks or unintended breaches (7). The existence of large amounts of data can also make it tempting to see it as property of the institution, making it easy to justify the querying, exposing, and selling of data without the consent of individuals (35).

Scope creep

Scope (or function) creep refers to the disclosure and use of personal data for purposes not related to the original intent of data collection, and without the informed consent of individuals (6). Examples include biometric data captured as part of enrolment into national ID systems that are then made accessible to law enforcement for surveillance, or personal data that are on-sold to private companies for commercial use, or agencies that request customers to provide their UIN to access services when there is no legal basis to do so (7). Concerns over scope creep have been raised in instances where national unique identifiers have gradually been adopted by various services and platforms for their own purposes, including identification, linking, and tracking (34, 49).

Operating environment

There are general concerns regarding the overall management and maintenance of the systems supporting the generation, assignment and use of unique identifiers (35). Concerns include the insecure or high-risk digital environments many electronic administrative systems operate in, and reliance on the private sector to provide telecommunications and financial infrastructure needed for the administration of electronic transfers, which can increase the risk of privacy and security breaches if not managed adequately (34). The diverse nature of many administrative information management systems using UINs, especially those established by development or humanitarian agencies, can also lead to issues of unclear roles and responsibilities regarding data ownership (and responsibility for system upkeep) – calling for better harmonization and the use of commonly agreed frameworks.

Common challenges are magnified in countries with limited supporting infrastructure, large rural populations, unreliable telecommunications, limited in-country capacity, and weak legislation on key data privacy and security issues (49). Key findings from a World Bank review of identification systems in Africa (33), for example, included the lack of adequate legal frameworks to support and regulate identity management systems, with overlapping or unclear mandates among various stakeholders, and a lack of sufficient regulations to protect personal data and uphold individuals' rights to privacy and the fair use of their data, with many identity-related laws outdated. In 2022, Human Rights Watch examined six systems built by private companies for or with the assistance of foreign governments and international institutions in Afghanistan, three of which were national identification systems. They identified several concerns relating to issues of data processing and security, data transmission and storage, and the possibility of data loss, noting that many of the systems were implemented before local data protection and privacy laws were enacted in the country (50).

Specific risks for people in vulnerable situations

Unique identifiers pose specific risks for people in vulnerable situations and groups at risk of marginalization,[4] including those relating to data protection and privacy, exclusion through system design or technology limitations and failures, and unintended uses of linked data. These individuals and groups are particularly vulnerable during the collection, analysis, and storage of their personal data, as they are often less aware of the risks and consequences of such processing, and of their rights and the safeguards in place to protect them (8). This is particularly concerning when considering children and young people, as more data will be collected on them over their lifetime than ever before, and the future use, application, and impact of such data remain largely unpredictable – making it difficult to assess potential harms and benefits in the 'best interests of the child' as required by Article 3 of the CRC, for example (51).

Overall, data collection, analysis, and regulation in the digital age requires more specific protection for people in vulnerable situations and groups at risk of marginalization, to ensure their rights are upheld, while also balancing the risks and opportunities of digital innovations (51).

The risks associated with the intentional misuse and/or design flaws of systems designed to generate, assign, and store unique identifiers for these individuals and groups include (6, 13, 33):

- **Exclusion from services, rights, and entitlements**. The formalization of identity systems and introduction of additional identification requirements, such as UINs, can increase the risk of exclusion, particularly when people have previously been able to provide their identities through alternative or informal means. As such, systems that cannot meet the needs of already marginalized populations, through failure or biases, may deepen inequalities. For instance, in countries where foundational systems lack coverage, functional systems have often moved to fill the gaps in identification, however these are often exclusive systems – often omitting children and non-citizens. Other marginalized groups, including children in street situations, and children who are (or whose parents are) stateless, internally displaced, migrants, refugees, or asylum seekers, may also disengage from services that require the collection of personal information such as UINs for fear of 'identification' by service providers, family members, the state, etc.

4 This includes, among others, women and girls, low-income and low-literacy populations, refugees, migrants, internally displaced persons (IDPs), stateless persons, persons with disabilities, and people of diverse sexual orientations and gender identities (SOGI).

- **Identity theft or fraud**, with personal data increasingly targeted by identity thieves and unique identifiers able to act as enablers for identity theft, with long-term effects for those affected. People in vulnerable situations and groups at risk of marginalization are often more vulnerable to identity theft, as they are less equipped to monitor what data are being collected about them and how it is being used, meaning that theft and fraud can go on undetected for longer periods of time.
- **Privacy violations**. The digital transmission, networked storage, and increased sharing of unique identifiers may expose personal information to others, placing it at risk of becoming public (or at least, shared beyond the conditions under which it was collected). Unique identifiers, by increasing the 'linkability' of previously independent datasets can also increase the risk of data being used against people's interests, such as for surveillance.
- **Loss of agency over the use of personal data**. People in vulnerable situations and groups at risk of marginalization can more rapidly lose agency (control) over the use of their data once linked across systems. This can make it more difficult to identify and remove their data from various databases, which can lead to unlawful processing – violating the principles of purpose specificity, proportionality, lawfulness, retention limitation, and the rights to access, request deletion and object against processing. As more data about the individuals and groups are generated by others (such as through the linking of different data sources), their ability to control their own personal data is further reduced.

The design of unique identifiers can have significant implications for migrant inclusion. India's Aadhaar system, though designed for broad inclusion, often excludes migrants lacking proof of permanent residence, limiting access to banking and social benefits. An inclusive system ensures that all individuals—regardless of nationality, legal status, or documentation—can obtain an identifier and access essential services. For instance, Mexico's Clave Única de Registro de Población (unique key of population registry) number is available to all residents, including irregular migrants, supporting school enrollment and access to emergency healthcare. Portugal allows migrants with a residence permit to obtain a Social Security Number and a National Health Service number, enabling access to healthcare and social services. Morocco issues a residence permit-linked unique identifier, granting foreign nationals with legal status access to public services, including banking and social programmes.

Linking identifiers across databases can expose migrants – especially those with irregular status – to surveillance and enforcement. In the United States, concerns have been raised about data-sharing agreements between local service providers and federal immigration authorities, where biometric and identity data collected for driver's licenses or social services have later been used for immigration enforcement actions. In Thailand, migrant workers must register in national labour databases to obtain work permits. However, this system has also been used to track and deport those who overstay their permits. Such practices deter migrants from accessing services, even when they are legally entitled to them.

Core principles for a good identifier

The characteristics that make a 'good' identifier depend, in part, on how it will be used – for example, as a national unique identifier to link data across sectors, or as a sector-specific identifier with a more limited scope. In general, a good identifier should be unique, universal, and stable, following the general points below (6, 10, 16, 18, 19, 52):

- **Uniqueness**. Each person should have only one unique identifier and each identifier must correspond to one and only one individual.
- **Inclusivity**. The system supporting the identifier should ensure that all individuals residing in a country, including all age groups, nationals and non-nationals, and marginalized or vulnerable populations, are included and can access their identifiers without barriers.
- **Timeliness**. The unique identifier should be assigned at birth (or as close to birth as possible), and linked with birth registration, particularly for foundational, national identifiers. Early assignment ensures inclusion from the earliest stages of life, efficient service delivery throughout life, and supports lifelong identity management.
- **Permanence**. The identifier should remain attached to the individual for their lifetime and should never be reassigned to another person, even after death or emigration. Unique identifiers should be retired upon death registration. This ensures continuity and prevents duplication or misuse.
- **Clarity and minimized ambiguity**. Whether represented in automated or handwritten form, the identifier should minimize the risk of misinterpretation (e.g., avoiding characters that can be confused, such as the letter 'o' and the number '0').
- **Validation and verification**. The identifier should be subject to validation through digital checks (e.g., checksum algorithms) or verification against base registers to ensure accuracy and prevent errors or fraud.
- **Scalability and future-proofing**. The identifier system should be designed to support every living person for the foreseeable future. This includes accommodating population growth and potential expansion to include non-residents or foreign nationals. The identifier should be compatible with current and emerging digital systems and technologies, enabling its use in online authentication, e-governance, and other digital services.
- **Randomization**. There is an increasing preference for random identifiers over coded or structured identifiers. Random identifiers provide a higher level of security by making it difficult to reconstruct or guess the identifier, thereby reducing the risk of unauthorized access and protecting personal information.
- **Interoperability**. The identifier should be compatible with multiple systems and sectors (e.g., healthcare, education, social welfare) to facilitate seamless data linkage and service delivery across different domains.
- **Privacy and security**. The identifier system should incorporate robust data protection measures, including encryption, tokenization, and access controls, to safeguard sensitive information and prevent misuse and fraudulent activities, such as identity theft.
- **Legal and regulatory compliance**. The identifier system should align with national and international data protection laws and standards, ensuring compliance with privacy regulations and building public trust. Clear communication and transparency about how the identifier is used, stored, and protected are essential to gaining public trust and encouraging widespread adoption (53).

Designing inclusive systems

Systems built on unique identifiers can become a source of exclusion if having a UIN becomes a (formal or de facto) requirement for service provision; if it is costly or difficult for individuals to obtain a UIN; if there are technical barriers that prevent the system from assigning and managing UINs effectively (such as limited connectivity); when UINs are only assigned to adults (e.g., those aged 18+ years); or as a direct result of government policy or action (for example, if identifiers are only provided to citizens) (7). Designing an inclusive system involves both the continued monitoring of information about individuals who have successfully obtained their UIN, in comparison with known information about the total population, people in vulnerable situations, and groups at risk of marginalization (54). Factors such as gender, age, income, ethnicity, religion, and geographic location are commonly known to have an impact on access, along with the additional barriers marginalized groups face such as cost, physical distance, different languages and cultures, discrimination, or legislative barriers.

Once the extent of potential inequalities in access and coverage has been established, strategies for inclusion need to be developed and implemented, including making sure alternative means of identification are accepted, and that individuals without a UIN are supported in obtaining one. The Ministry of Education in Jordan, for instance, modified its education management system to allow Syrian children to enroll in Jordanian schools using their refugee registration number as provided by UNHCR's digital Population Registration and Identity Management Ecosystem (PRIMES), in place of the national ID number provided to Jordanian citizens. Strategies for inclusion can also include setting different targets, such as in Indonesia, where the Ministry of National Development Planning (BAPPENAS) has set a specific target for birth certificate ownership of children from the poorest households, as they currently have some of the lowest rates of birth registration (55).

Ensuring data protection and privacy

While a strong legislative framework is critical when implementing or updating systems of unique identifiers, there are several other approaches that can be taken to ensure the protection and privacy of personal data (also referred to as personally identifiable information, or PII). These include the data processing principles, as defined by the General Data Protection Regulation (GDPR) (56), and the OECD Privacy Guidelines (57), among others. Overall, these guidelines emphasize the importance of privacy and data protection in ensuring trust in the collection and use of data, and in ensuring that government access to such data is not unconstrained or unreasonable.

Organizational, administrative, physical, and technical safeguards and procedures to ensure data protection and privacy include anonymization, pseudonymization, encryption and conditional pseudonymity (data minimization). Countries are increasingly incorporating technological advances such as tokenization for ensuring data protection and privacy (see **Box 2**), which has the advantage that, by *replacing* personal data, it is impossible to recover the original data in the case of a data breach (7). One such example is India's Aadhaar Virtual ID (VID), a temporary, 16-digit code linked to an individual's Aadhaar number. Introduced by the Unique Identification Authority of India, the feature allows Aadhaar holders to authenticate their identity without revealing their actual Aadhaar number or other sensitive details. The VID can be used for a variety of purposes including opening a bank account, applying for government services, accessing government subsidies, and applying for a passport (58).

BOX 2

SERVICE-SPECIFIC IDENTIFIERS AND TOKENIZATION

The data contained on Austria's virtual citizen card (CC) includes an individuals' full name, date of birth, cryptographic keys required for encryption and digital signatures, and the 'SourcePIN' – a unique identifier created by encryption of the 12-digit unique ID (CCR) number. To ensure privacy, the eGovernment Act states that different unique identifiers must be used for each of the country's 26 public administrative sectors, such as health, education, taxation, etc.

A sector-specific personal identifier (ssPIN) is created from the SourcePIN using a one-way process (tokenization). Unlike the SourcePIN, the ssPIN can be stored in administrative databases. Public authorities can use the same ssPIN to retrieve an individual's data stored within the same sector to view records, or pre-fill forms. However, authorities cannot access the ssPINs from other sectors.

For more information see:

ID4D Practitioner's Guide (2019)

Available here



7 REFERENCES

1. McMurry JA, Juty N, Blomberg N, Burdett T, Conlin T, Conte N, et al. Identifiers for the 21st century: How to design, provision, and reuse persistent identifiers to maximize utility and impact of life science data. PLoS Biol. 2017;15(6):e2001414-e. DOI: https://doi.org/10.1371/journal.pbio.2001414.
2. ID4D Practitioner's Guide: Version 1.0. Washington, DC: World Bank; 2019 (https://id4d.worldbank.org/guide).
3. United Nations Legal Identity Expert Group. Implementation of the United Nations Legal Identity Agenda. United Nations Country Team. Operational Guidelines. United Nations Development Programme, United Nations Statistics Division, United Nations Children's Fund; 2020 (https://unstats.un.org/legal-identity-agenda/documents/UNCT-Guidelines.pdf).
4. The role of digital identification for healthcare: The emerging use cases. Washington, DC: World Bank; 2018 (https://documents.worldbank.org/en/publication/documents-reports/documentdetail/595741519657604541/the-role-of-digital-identification-for-healthcare-the-emerging-use-cases).
5. Algoso D, Drury P, Hammer S. Identifying and addressing risks to children in digitised birth registration systems: A step-by-step guide. Surrey, UK: Plan International; 2015 (https://getinthepicture.org/resource/plan-international-digital-birth-registration-risk-assessment-tool).
6. United Nations Statistics Division. Guidelines on the legislative framework for civil registration, vital statistics and identity management systems. New York: UNSD, Department of Economic and Social Affairs, Statistics Division; 2023 (https://desapublications.un.org/publications/guidelines-legislative-framework-civil-registration-vital-statistics-and-identity).
7. Asia-Pacific Guidelines to Data Integration for Official Statistics. Bangkok: United Nations Economic and Social Commission for Asia and the Pacific; 2021 (https://www.unescap.org/sites/default/d8files/knowledge-products/Data_Integration_Guidelines_ESCAP.pdf).
8. Organisation for Economic Co-operation and Development. OECD Glossary of Statistical Terms 2021 (https://stats.oecd.org/glossary/detail.asp?ID=1274).
9. The Centre for Humanitarian Data. Glossary. United Nations Office for the Coordination of Humanitarian Affairs; 2021 (https://centre.humdata.org/glossary/).
10. Clark J, Dahana M, Desaia V, Iencob M, Labriollec Sd, Pellestorc J-P, et al. Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation. A joint World Bank Group – GSMA – Secure Identity Alliance Discussion Paper. Washington, DC: The World Bank Group, GSMA, and Secure Identity Alliance; 2016 (https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-for-development/wp-content/uploads/2016/07/Towards-Shared-Principles-for-Public-and-Private-Sector-Cooperation.pdf).

11. Guidance on the protection of personal data of persons of concern to UNHCR. Geneva: United Nations High Commissioner for Refugees, Division of International Protection; 2018 (https://www.refworld.org/policy/opguidance/unhcr/2018/en/121076).

12. UNICEF Procedure for Ethical Standards in Research, Evaluation and Data Collection and Analysis. Office of Research. New York: United Nations Children's Fund; 2021 (https://www.unicef.org/evaluation/documents/unicef-procedure-ethical-standards-research-evaluation-data-collection-and-analysis).

13. Recommendations for a Unique Health Identifier for Individuals in Ireland. Mahon, Cork: Health Information and Quality Authority; 2009 (https://www.hiqa.ie/sites/default/files/2017-02/Unique_Health_Identifier_Report%20(1).pdf).

14. Digital Identity Toolkit. A guide for stakeholders in Africa. Washington, DC: The World Bank Group; 2014 (https://documents.worldbank.org/en/publication/documents-reports/documentdetail/147961468203357928/digital-identity-toolkit-a-guide-for-stakeholders-in-africa).

15. Using administrative and secondary sources for official statistics: A handbook of principles and practices. Geneva: United Nations Economic Commission for Europe; 2011 (https://unece.org/DAM/stats/publications/Using_Administrative_Sources_Final_for_web.pdf).

16. Dygaszewicz J. Undertaking population and housing censuses. Register-based and combined methodologies. Beirut: Economic and Social Commission for Western Asia; 2018 (https://www.unescwa.org/sites/default/files/pubs/pdf/undertaking_population_and_housing_census_register-based_and_combined_methodologies.pdf).

17. Integrating unique identification numbers in civil registration. Washington, DC: World Bank; 2016 (https://thedocs.worldbank.org/en/doc/795091518546134883-0090022018/original/Integrating-UniqueIdentification.pdf).

18. Mathenge G, Nahmias P, Sejersen T, Yazdani A. Population registers: A key resource for producing vital statistics. Bangkok, Thailand: United Nations Economic and Social Commission for Asia and the Pacific; 2020 (https://repository.unescap.org/handle/20.500.12870/953).

19. Compendium of good practices in identity management in the OSCE region. Warsaw: Organization for Security and Co-operation in Europe, Office for Democratic Institutions and Human Rights; 2017 (https://www.osce.org/odihr/346906).

20. Riplinger L, Piera-Jiménez J, Dooling JP. Patient Identification Techniques – Approaches, Implications, and Findings. Yearb Med Inform. 2020; 29(1): 81-6. DOI: https://doi.org.10.1055/s-0040-1701984.

21. Office of the Victorian Information Commissioner. IPP 7 – Unique identifiers. 2019 (https://ovic.vic.gov.au/book/ipp-7-unique-identifiers/#'Unique_identifiers).

22. Register-based statistics in the Nordic countries. Review of best practices with a focus on population and social statistics. Geneva: United Nations Economic Commission for Europe; 2007 (https://unece.org/fileadmin/DAM/stats/publications/Register_based_statistics_in_Nordic_countries.pdf).

23. MacFeely S, Dunne J. Joining up public service information: The rationale for a national data infrastructure. Administration. 2014; 61(4): 93–107 (https://cora.ucc.ie/server/api/core/bitstreams/6922dd4d-ba6f-4863-a2a2-d9dde070a4af/content).

24. Data integration manual: 2nd edition. Wellington: Statistics New Zealand; 2015 (https://stats.govt.nz/assets/Uploads/Integrated-data-infrastructure/Your-information-in-the-IDI/Data-Integration-manual-2nd-edition.pdf).

25. Casher C, Metz A and Clark J. ID4D Global Dataset Volume 3: Trends in Identification for Development. Washington, DC: World Bank; 2024 (https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099031924132035631/p17634114229a80dc18ea11c4c279817517).

26. Legal identity systems in Asia and the Pacific: Civil registration, vital statistics, and identity management. ESCAP/MCCRVS/2021/INF/4. Bangkok: Economic and Social Commission for Asia and the Pacific; 2023 (https://www.unescap.org/kp/2023/legal-identity-systems-asia-and-pacific-civil-registration-vital-statistics-and-identity).

27. Mills S, Lee JK, Rassekh BM, Kodelja MZ, Bae G, Kang M, Pannarunothai S and Kijsanayotin B. Unique health identifiers for universal health coverage. Journal of Health, Population and Nutrition. 2019; 38(S1): 22. DOI: https://doi.org/10.1186/s41043-019-0180-6.

28. Using unique identifiers for person-centred monitoring of HIV services. Consolidated guidelines on person-centred HIV patient monitoring and case surveillance. Geneva: World Health Organization; 2017 (https://www.who.int/publications/i/item/978-92-4-151263-3).

29. Privacy Act 2020. Public Act No. 31, Version as at 1 July 2024. Wellington: Parliamentary Counsel Office, Ministry of Justice; 2024 (https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html?search=sw_096be8ed81e6756a_unique+identifier_25_se&p=1#LMS23376).

30. Guidelines to the Information Privacy Principles (IPP): IPP 7 - Unique identifiers. Melbourne: Office of the Victorian Information Commissioner; 2019 (https://ovic.vic.gov.au/book/ipp-7-unique-identifiers/).

31. National Community Services Information Management Group. Statistical data linkage in community services data collections. Canberra, Australia: Australian Institute of Health and Welfare; 2004 (https://www.aihw.gov.au/reports/technical-report/statistical-data-linkage-community-services-data/contents/table-of-contents).

32. Considerations and guidance for countries adopting national health identifiers. Geneva: Joint United Nations Programme on HIV/AIDS and United States President's Emergency Plan for AIDS Relief; 2014 (https://www.unaids.org/en/resources/documents/2014/national_health_identifiers).

33. Clark J. The state of identification systems in Africa. Washington, DC: World Bank; 2017 (https://documents1.worldbank.org/curated/en/156111493234231522/pdf/114628-WP-68p-TheStateofIdentificationSystemsinAfricaASynthesisofIDDAssessments-PUBLIC.pdf).

34. Hosein G, Nyst C. Aiding surveillance. An exploration of how development and humanitarian aid initiatives are enabling surveillance in developing countries. 2013 (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2326229).

35. Aggarwal N, Ben-Hassine W, Chima R. National digital identity programmes: What's next? Policy Paper. New York: Access Now; 2018 (https://www.accessnow.org/wp-content/uploads/2019/11/Digital-Identity-Paper-Nov-2019.pdf).

36. Barbosa GCG, Ali MS, Araujo B, Reis S, Sena S, Ichihara MYT, et al. CIDACS-RL: a novel indexing search and scoring-based record linkage system for huge datasets with high accuracy and scalability. BMC Medical Informatics and Decision Making. 2020; 20(1): 289. DOI: https://doi.org/10.1186/s12911-020-01285-w.

37. Andrew NE, Sundararajan V, Thrift AG, Kilkenny MF, Katzenellenbogen J, Flack F, et al. Addressing the challenges of cross-jurisdictional data linkage between a national clinical quality registry and government-held health data. Aust N Z J Public Health. 2016; 40(5): 436–442. DOI: https://doi.org/10.1111/1753-6405.12576.

38. van Langenhove T, Suchonwanich N, Schmitt V, Ortiz I and Sakunphanit T. Thailand: A national health insurance beneficiary registry based on national identification numbers. International Labour Office, Social Protection Department; 2015 (https://researchrepository.ilo.org/esploro/outputs/995218906302676).

39. Raab G. Education data available within the Scottish Longitudinal Study. Fife, Scotland: University of St Andrews; 2013 (https://calls.ac.uk/output-entry/education-data-available-within-the-scottish-longitudinal-study/).

40. Stewart CH, Dundas R, Leyland AH. The Scottish school leavers cohort: linkage of education data to routinely collected records for mortality, hospital discharge and offspring birth characteristics. BMJ Open. 2017; 7(7): e015027 (https://bmjopen.bmj.com/content/7/7/e015027).

41. Connelly G. The Educational Attainment of Looked After Children: Scottish Government Policy. Glasgow: University of Strathclyde; 2010 (https://pure.strath.ac.uk/ws/portalfiles/portal/66009552/looked_after_children_scottish_government_policy.pdf).

42. Adjei J, Olesen H. Building trusted national identity management systems: Presenting the privacy concern-trust (PCT) model. CENTRIC 2012: Lisbon, Portugal, 18–23 November 2012 (https://vbn.aau.dk/en/publications/building-trusted-national-identity-management-systems-presenting-).

43. Managing Patient Identity Across Data Sources. In: Gliklich R, Dreyer N, Leavy M, editors. Registries for Evaluating Patient Outcomes: A User's Guide, 3rd edition. Rockville, MD: Agency for Healthcare Research and Quality; 2014 (https://pubmed.ncbi.nlm.nih.gov/24945055/).

44. Christen P. Data Linkage: The Big Picture. Harvard Data Science Review. 2019; 1(2). DOI: https://doi.org/10.1162/99608f92.84deb5c4.

45. Asher J, Resnick D, Brite J, Brackbill R, Cone J. An Introduction to Probabilistic Record Linkage with a Focus on Linkage Processing for WTC Registries. International journal of environmental research and public health. 2020; 17(18): 6937. DOI: https://doi.org/10.3390/ijerph17186937.

46. Bohensky MA, Jolley D, Sundararajan V, Evans S, Pilcher DV, Scott I, et al. Data Linkage: A powerful research tool with potential problems. BMC Health Services Research. 2010; 10(1): 346. DOI: https://doi.org/10.1186/1472-6963-10-346.

47. Sadhya D & Sahu T. A critical survey of the security and privacy aspects of the Aadhaar framework. Computers & Security. 2024; 140: 103782. DOI: https://doi.org/10.1016/j.cose.2024.103782.

48. Netter WJ. Curing the unique health identifier: A reconciliation of new technology and privacy rights. Jurimetrics. 2003; 43(2): 165–186 (https://pubmed.ncbi.nlm.nih.gov/15156882/).

49. Zelazny F. The Evolution of India's UID Program: Lessons Learned and Implications for Other Developing Countries. CGD Policy Paper 008. Washington, DC: Center for Global Development; 2012 (https://www.cgdev.org/publication/evolution-india%E2%80%99s-uid-program-lessons-learned-and-implications-other-developing).

50. New evidence that biometric data systems imperil Afghans. New York: Human Rights Watch; 30 March 2022 (https://www.hrw.org/news/2022/03/30/new-evidence-biometric-data-systems-imperil-afghans).

51. Berman G and Albright K. Children and the Data Cycle: Rights and Ethics in a Big Data World. Florence: UNICEF Office of Research; 2017 (https://www.researchgate.net/publication/320516771_Children_and_the_Data_Cycle_Rights_and_Ethics_in_a_Big_Data_World).

52. Standard guide for properties of a universal healthcare identifier (UHID). ASTM E1714-07(2013). West Conshohocken: ASTM International; 2013 (https://www.astm.org/e1714-07r13.html, *withdrawn 2022*).

53. Inequality assessment. Bangkok: Economic and Social Commission for Asia and the Pacific; 2019 (https://getinthepicture.org/regional-picture/implementation-steps/inequality-assessment).

54. Module 4.3: Information campaigns. UNHCR Guidance on registration and identity management (https://www.unhcr.org/registration-guidance/chapter4/information-campaigns/).

55. Civil registration and vital statistics as an accelerator for implementing the 2030 Agenda for Sustainable Development and ensuring that no one is left behind. ESCAP/MCCRVS/2021/4. Bangkok: Economic and Social Commission for Asia and the Pacific; 2021 (https://www.unescap.org/sites/default/d8files/event-documents/ESCAP_MCCRVS_2021_4_CRVS_as_an_accelerator_English.pdf).

56. Article 5 – Principles relating to processing of personal data. General Data Protection Regulation (GDPR). Brussels: European Union, Horizon 2020 Framework Programme; 2024 (https://gdpr.eu/article-5-how-to-process-personal-data/).

57. OECD Privacy Guidelines. Paris: Organisation for Economic Co-operations and Development; 2025 (https://www.oecd.org/en/topics/policy-issues/privacy-and-data-protection.html).

58. Virtual ID (VID). Delhi: Unique Identification Authority of India, Government of India; 31 January 2025 (https://uidai.gov.in/en/contact-support/have-any-question/284-english-uk/faqs/aadhaar-online-services/virtual-id-vid.html).

For more information, please visit:

getinthepicture.org

Statistics Division

United Nations Economic and Social Commission for Asia and the Pacific

United Nations Building
Rajadamnern Nok Avenue
Bangkok 10200, Thailand

escap-crvs@un.org

unicef
for every child

ESCAP
Economic and Social Commission for Asia and the Pacific

Get every one in the picture