# Identifying and addressing risks to children in digitised birth registration systems:

**a step-by-step guide**

Plan

**Plan**

International Headquarters
Dukes Court
Duke Street
Woking
Surrey GU21 5BH
United Kingdom

t +44 (0) 1483 755155

f +44 (0) 1483 756505

**plan-international.org/birthregistration**

Plan

# Acknowledgements

This publication was produced by Reboot and the Commonwealth Telecommunications Organisation on behalf of Plan International's Digital Birth Registration Team.

**Authors:** Dave Algoso, Peter Drury and Samantha Hammer (Reboot)

**This report benefited from the expertise, continued support and technical assistance of the following Plan staff:**

Edward Duffus, Global Digital Birth Registration Manager, Plan IH

Giorgiana Rosa, (former) Head of Policy, Plan IH

Nicoleta Panta, Global Count Every Child Advocacy Manager, Plan IH

Matt Crook, Communications Consultant

**The following have been instrumental in the consultation and review process of the report and helped shape the guide to its final form:**

Willian C Philbrick, Innovations and Child Protection Program Lead, UNICEF

Carly Nyst, Legal Director, Privacy International

Seth Chilton, Technology for Development Consultant, UNICEF

Sophie Taylor, Programme Lead – Civil Registration and Vital Statistics, De la Rue

Mia Harbitz, Lead Specialist, Registries, IFD/ICS, Inter-American Development Bank

Mark Landry, Coordinator, Health Intelligence and Innovation, World Health Organisation, Western Pacific Regional Office

Matthew Perkins, Economic Affairs Officer, ICT and Development Section, United Nations Economic and Social Commission for Asia and the Pacific

**The expertise and knowledge of a special reference group enhanced this report:**

Francis C. (Sam) Notzon, Director of the International Statistics Program at the National Center for Health Statistics, Centers for Disease Control and Prevention

Frank Odhiambo, KEMRI/ Centers for Disease Control and Prevention HDSS Branch Chief, KEMRI-CGHR, Kisumu, Kenya

Laila El Baradei, Legal Counsel, Plan International

Jenny Wang, Technical Consultant, Accenture ADP

Peter Njuguna, Digital Birth Registration Adviser, Plan International Kenya

Joan McCalla, retired, formerly Cisco

Prakash Kumar, Cisco, India

Joan Dzenowagis, World Health Organisation, Geneva

Andrew Bell, Business Consultant, Mobile Identity, Groupe Speciale Mobile Association

Tim Hayward, Senior Director, Operations, Caribou Digital

Eddie Turnbull, Head of eHealth, Scotland

Clare Sanderson, Director of Solution Design, Standards and Assurance, Health and Social Care Information Centre

Asim Hussain, Director of Strategy for Service Ontario

Professor David Wall, University of Durham

Design:Joely Merrington

Proofreading: Paula McDiarmid


JESSICA LOMELIN/PLAN INTERNATIONAL

# Contents

# Executive summary

Incorporating digital technologies in birth registration processes holds important potential for expanding the reach of registration and its benefits. This potential is beginning to be realised in a few countries: birth registration efforts through mobile phones have been linked to increasing registration rates in Uganda,[1] and web-enabled birth registration in Uruguay allows newborns to receive their birth certificates before they leave the hospital.[2] As countries expand their e-government capacities, digitised birth registration (DBR) may support governments in fulfilling their responsibility for civil registration and the provision of vital statistics.

Success stems from the ability of digital technology to streamline registration processes and improve data quality, overcoming both the geographic and bureaucratic barriers that often keep registration low. However, as with the introduction of any new technology, there are also potential dangers. These dangers have received little attention to date. To avoid them, implementing government agencies and their partners need to understand the potential for harm related to DBR in general, and how to assess this potential in their specific country context. When the risks are mitigated, the full value and benefits of digital technologies in birth registration can be realised.

This document provides guidance on identifying and mitigating these risks for implementing government agencies and their partners operating in low- and middle-income countries. It expands on the model of DBR developed by Plan International as part of its Count Every Child initiative and within the context of strengthening civil registration and vital statistics (CRVS) systems more broadly.

## Child protection threats

Although introducing electronic processes to birth registration offers important security benefits – including greater accountability, improved data quality, and reduced data loss – it does not eliminate all child protection threats that may come about through birth registration.

Intentional misuse of data and/or unintentional design flaws can result in threats to child protection. These include:

1. Identity theft or fraud. Personal data, including that of children, is increasingly in demand by identity thieves. Digitised data may be easier for tech-savvy thieves to steal in large quantities.
2. Privacy violation. Digital transmission, networked storage and increased sharing of birth data may expose personal information to individuals and uses that are against the wishes of families participating in registration.
3. Targeting based on personal characteristics. The ability to rapidly gather and process large amounts of population data could contribute to targeted advertising or other forms of exploitation.

4. Personal security violation or exploitation. Registration happening outside a controlled institutional environment, such as a hospital or registrar's office, could place families at risk of physical violence and economic or other exploitation by registration agents.
5. Exclusion from the benefits of birth registration. While digitisation can extend registration benefits to previously marginalised populations, systems that cannot meet the needs of the already marginalised may deepen inequalities.

These threats to children may originate through any number of factors present in the design and implementing context of a birth registration system that uses digital technologies. These risk factors fall into two categories: those that cut across all elements of a birth registration system, and those that arise from particular steps in a registration process.

## Mitigating risks across a digitised birth registration system

An agency seeking to create or improve a digitised birth registration system should consider the risk factors that cut across all steps in the birth registration process before engaging in a particular context. This starts with system-wide risks that are not easily addressed, then moves to those that are more open to mitigation.

1. Operating environment. Risks in the operating environment relate to the social and institutional context, the legal framework, and the institutional positioning of birth registration. Legal reform efforts can be undertaken to mitigate some of these risks, but others are harder to move.
2. Stakeholders. System-wide risks relating to the stakeholders generally include partner coordination and involvement. Important stakeholders include leading government agencies and technology implementers as well as the families who are meant to benefit from birth registration. These risks can be mitigated largely through good project management in the system design process and roll-out.
3. Information and identity management. Poor information and identity management raises the risk that unauthorised users access the birth registration system and that data becomes corrupted or misused. Implementing a strong information governance framework and instituting multiple electronic and manual identity checks on all participants are two important mitigation mechanisms.

## Mitigating risks in each step of a digitised birth registration process

In addition to the broad risks to be addressed by system-wide mitigations, each step of a birth registration process brings with it specific risks that should be accounted for in system design. For example, where collection of birth registration data is concerned, there exists a risk that caregivers may not understand how the collected data will be used. System designers can mitigate against this by creating context-appropriate informed consent practices. In this same way, further risks and possible mitigations will be explored in detail in this document, providing guidance for the design and implementation of a digitised birth registration process.


JESSICA LOMELIN/PLAN INTERNATIONAL

# Glossary

**Child protection threat:** Child protection efforts support the right of all children to live free from violence, abuse, neglect, and exploitation. Threats to child protection can be due to actions that result in actual or potential harm to a child, as well as due to failures to act which, intentionally or unintentionally, harm a child or damage their wellbeing, dignity and prospects of safe and healthy development into adulthood. This document focuses on the child protection threats which may come about in the context of digitised birth registration.

**Digitised birth registration (DBR):** According to UNICEF, birth registration is "the continuous, permanent and universal recording, within the civil registry, of the occurrence and characteristics of births in accordance with the legal requirements of a country".[3] DBR employs digital technology to facilitate collection, processing, storing, and/or sharing of birth data. The generic model of DBR included in this document builds on the model being developed by Plan International, but is context- and technology-neutral and therefore addresses a number of possible real-world models.

**Identity theft:** Identity fraud occurs when a person or organisation comes into possession of, uses, or shares an individual's personal data to commit fraud or another crime.[4]

**Information governance:** Information governance comprises the system by which an organisation manages information and data. Drawing on principles of data management, business process management, and risk management, an information governance scheme defines the authority and decision-making structures around the optimisation, security, quality, and use of data.[5]

**Personal data:** Personal data includes anything that identifies or can be used to identify a living individual, either directly or indirectly. In the context of DBR, this involves birth data that is gathered, transmitted, stored or otherwise processed using electronic devices.

**Privacy:** Privacy and confidentiality are fundamental rights, but are also relative concepts that vary by context. For this document, we employ the definition used to describe the right to privacy in Article 17 of the International Covenant on Civil and Political Rights, which states that "privacy" means that "1.) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2.) Everyone has the right to the protection of the law against such interference or attacks."[6] We assess the extent to which DBR implementations threaten or protect privacy based on standards established in the European Union Data Protection Directive, which strictly limits collection, use, and exposure of personal data, requiring that such actions represent a legitimate purpose and meet conditions for safety and security.[7]

## Technology-related terms

| | |
|---|---|
| Application Programming Interface (API): | An API can take many forms, but at the core it is a "set of commands, functions, and protocols" that a programmer develops to create software applications and allow them to interact.[8] |
| Cloud storage: | Cloud storage systems are publicly or privately owned and administered servers (computer hardware and software) that are connected to a network and are used to store and share data.[9] |
| Digital signature: | A digital signature is a unique string of data that can be reliably linked to a specific individual and used to sign or authenticate an electronic document. It depends on its user having a digital identity that has been externally verified by a certification authority.[10] |
| Public Key Infrastructure (PKI): | A PKI is a security measure to protect data that is shared over an insecure network. It relies on a trusted authority to authenticate users and grant them a specific "key" (a unique string of data associated only with that individual) that identifies them when they send and receive data. Many different PKI services and models are available.[11] |
| Short Message Service (SMS): | SMS is a widely used service that sends text messages to and between mobile phones via a mobile network operator. Messages can generally be up to 160 characters in length and can be stored on phones. |
| Unstructured Supplementary Service Data (USSD): | USSD is a protocol that allows mobile phones to exchange data with applications on a GSM network. Unlike SMS, USSD can only be sent during a defined session, and messages are not stored on the phones. It is commonly used to allow mobile subscribers to check account balances, or as part of mobile banking services. |

JESSICA LOMELIN/PLAN INTERNATIONAL

# 1. Introduction: digitising birth registration

Birth registration is central to the humanitarian goals of children's rights advocates worldwide. It paves the way toward a child's official identity, and constitutes a central right to be ensured by national governments.[12] For the role it plays in allowing governments to plan for and deliver public services, birth registration is increasingly recognised as a fundamental component of Civil Registration and Vital Statistics systems.

In developed and developing countries alike, digital and mobile technologies have the potential to streamline registration processes and improve data quality, contributing to higher registration rates and increased coverage. Uganda provides one example of a relatively low-registration context in which practitioners are implementing a mobile phone-based registration programme to raise birth registration rates.[13]

However, as with any new technology, the promise of digitised birth registration (DBR) cannot be realised without acknowledging the corresponding potential for harm. Birth data increasingly has value sought by individuals and groups who may use it to perpetrate fraud or other harm. Unaddressed risks that have the potential to produce negative outcomes for children and caregivers reduce the benefits offered by DBR initiatives, and potentially reduce the incentive for registration.

Governments, humanitarian practitioners, and others have developed measures to respond to risks as they evolve. This is an ongoing challenge, as motivated and tech-savvy individuals will continue to crack the toughest security walls and seek to exploit systemic weaknesses to get at valuable data.

Therefore, embarking on a DBR project requires a firm grasp of potential threats and an understanding of the mechanisms that may prevent them from occurring. It is also important for implementing institutions and system designers to think beyond technology-based factors by considering how the combination of technology, contextual factors, and the human element determine the most salient potential threats.

## 1.1 About this document

As an international child-centred community development organisation, Plan is fully committed to ensuring the fulfilment of children's rights, including their right to protection, as affirmed in the United Nations Convention on the Rights of the Child. Plan's Child Protection Policy commits the organisation and its associates to do everything within their control to rigorously assess and reduce risks to children in all operations, programmes and activities, and to take appropriate actions to report and respond to child protection concerns.

An expression of Plan's mandate, this document seeks to support low- and middle-income country governments in providing children with the benefits of DBR, informing practitioner's decision-making around the design and

implementation of DBR systems. It expands on the model of DBR developed by Plan International as part of its Count Every Child initiative and within the context of strengthening civil registration and vital statistics (CRVS) systems more broadly.

Several questions guided the enquiry underpinning this document:

1. What are the potential child protection threats that may arise through DBR?
2. How do contextual factors such as the legal frameworks, actors, processes, and tools involved determine which threats are most relevant in a given DBR system?
3. How can these threats be assessed by identifying risks across the system and at individual steps in the birth registration process?
4. How can these risks be mitigated?
5. Where current birth registration practice does not offer solutions, what analogous processes provide useful examples for thinking about potential risks and mitigation approaches?

With these questions in mind, this document starts by introducing the actors, processes, and tools that are common in DBR models, followed by the major related child protection threats. The nascent nature of the DBR field calls for a forward-looking assessment that considers threats that have actually been realised as well as those that could reasonably occur.

This document analyses the ways in which these threats may materialise in DBR implementation. These start with the system-wide risk factors related to the operating context, stakeholders, and management, as well as accompanying mitigation strategies. The analysis then turns to risks that are specific to each step in the DBR process. For both sets of risks, mitigation strategies are drawn from observed and extrapolated best practices to provide potential responses.

# 2. Elements of DBR

Birth registration digitisation may introduce new elements to traditional registration systems. These include technology tools used for birth notification, birth data collection, record storage, and birth record data sharing. In order to facilitate safe use of these technologies, digitised birth registration also introduces new processes and actors that carry their own risks. Understanding the tools, actors, and processes that are used in various DBR models is critical to understanding the risks faced in a particular implementation.

## 2.1 Tools

Two categories of tools form the technological backbone for DBR:

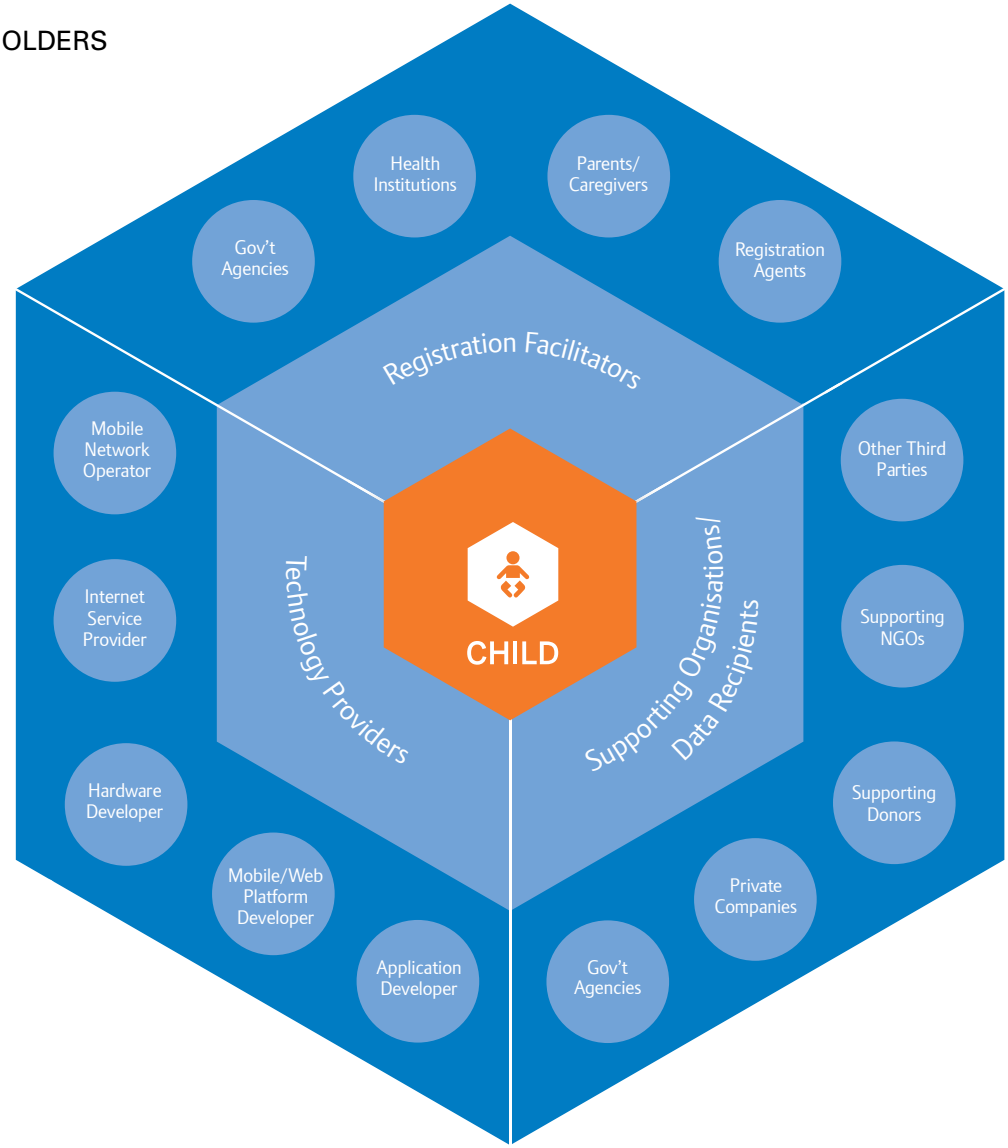
1. Devices and hardware. These include mobile phones (whether smartphones, feature phones, or 'dumb' phones), tablets, laptops, desktop computers, and physical servers.
2. Platforms and software components. These include: data transfer technologies, such as short message service (SMS), unstructured supplementary service data (USSD) or internet, sent through mobile phone or web-based forms; software interfaces, such as Application Programme Interfaces (APIs); and other back-end components, such as application and database software, and virtual storage.

While the technology component is the central feature of DBR, it functions within a host of programmatic, regulatory, outreach, and advocacy components that constitute an integrated DBR programme.

## 2.2 Stakeholders

Beyond the child who is meant to benefit from birth registration, a variety of other stakeholders – institutions, agencies, organisations and individuals – are involved. In Figure 1 below, these stakeholders are displayed according to their roles in a DBR system, as registration facilitators, technology providers and supporting organisations/data recipients.

*FIGURE 1*
DBR STAKEHOLDERS




### Registration facilitators

The registration process is facilitated at the lowest level by midwives, community health workers, village chiefs, doctors, nurses, health facility administrators, civil registry officials, mobile registration teams and others. In addition, health institutions and various government agencies (especially the Civil Registry Authority) are involved at a higher level of administration. Finally, parents/caregivers are also key facilitators.

### Technology providers

The tools mentioned in 2.1 rely on mobile network operators, internet service providers, mobile/ web platform developers, application developers, and hardware developers.

### Supporting partners/data recipients

Finally, various stakeholders may be involved in establishing DBR processes, promoting use of DBR, and accessing the resulting data. These include government agencies, supporting UN agencies, non-governmental organisations (NGOs), donors and private companies.

## 2.3 Digital birth registration process

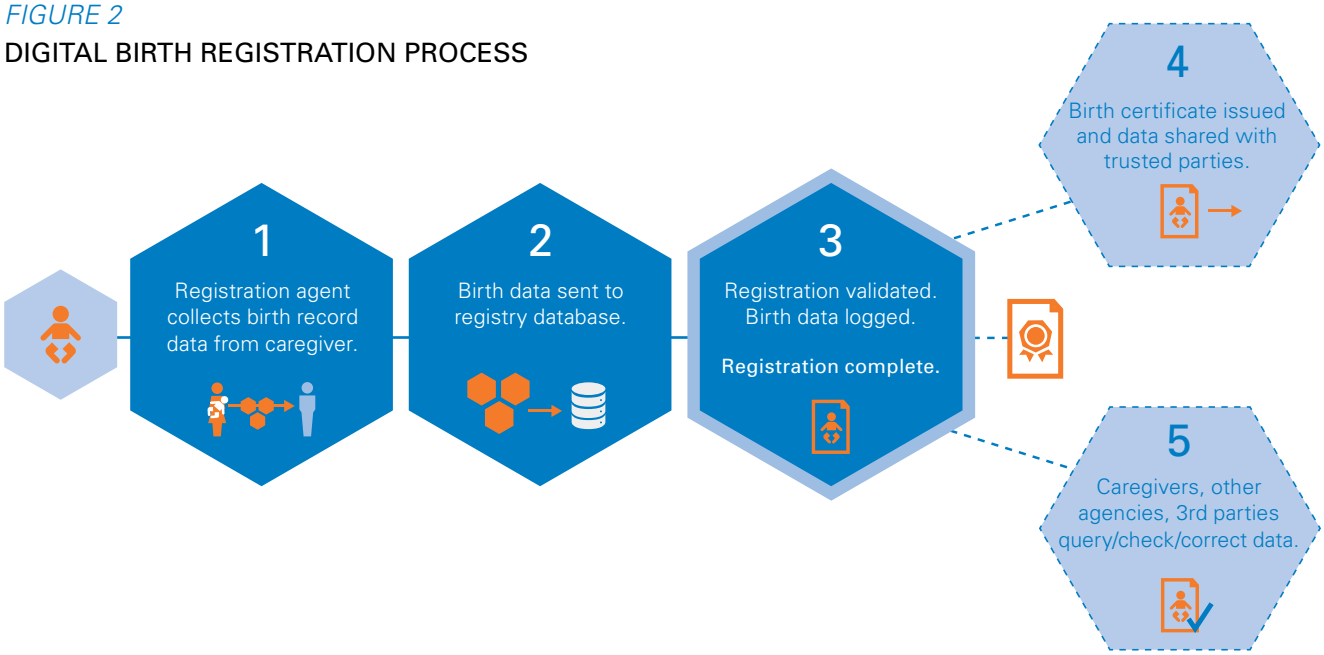
In general, a digitised birth registration process follows these steps:

1. The registration process begins with the parent, caregiver, healthcare provider, a village chief, or other individual informing a registration agent that a child has been born. The agent then collects the relevant birth data.
2. Once the necessary data to create a birth record has been collected the registration agent submits this data to the registrar.
3. The registrar then validates the data, the birth record is created and a birth certificate is issued to caregivers, finalising and affirming the registration. Depending on the specific DBR process being followed, a birth certificate may be issued to caregivers immediately once the birth record has been created and verified, or later, once additional validation has been done. Mobile and digitised birth registration processes allow for greater flexibility in the delivery format and timing of the birth certificate as well, with each variation carrying its own risks and potential mitigations. Discussing those variations is outside of the scope of this document, which analyses the registration process itself.
4. After the birth record is created, data is made available for sharing with trusted parties.
5. The process ends at the point where the birth data is able to be queried, corrected, and/or amended by parents, caregivers, or others (depending on their authority).

The following process map (Figure 2) illustrates how these steps connect in a typical DBR process.

*FIGURE 2*

DIGITAL BIRTH REGISTRATION PROCESS



JESSICA LOMELIN/PLAN INTERNATIONAL

### Variations around our simplified model

The generic model of DBR that this document considers is digitised at each step. It combines features of several existing DBR implementations, considers multiple possible devices, and encompasses processes of both institution-based and mobile-based DBR to enable a comprehensive discussion of DBR-related risks. Where relevant, this document notes risks that are most relevant to a particular variation of the model.

# 3. Potential threats to child protection

By streamlining registration processes and allowing for tighter data auditing, among other benefits, implementing a well-designed DBR system has the potential to make birth registration more effective. Even so, the introduction of a digital component may increase the potential for some child protection threats to occur.

Generally speaking, these threats are already present in traditional birth registration. In DBR, these threats may come about from either intentional wrongdoing or 'passive' harm related to inappropriate design or incorrect implementation. The threats described below include dangers that have been shown to link to the digitisation of birth data, processes with features similar to those of DBR, and dangers that analysis suggests have a reasonable potential to materialise.

The extent to which these threats are significant for a given DBR system depends on the context and the specifics of the system design. Before moving forward with DBR design and implementation, the implementing institution should carefully analyse the potential for these threats to emerge compared to the expected benefits of DBR and the threats posed by maintaining the current system.

## 3.1 Identity theft or fraud

Identity theft or fraud is one of the most salient child protection threats posed by participation in DBR. Identity thieves are keen to access birth registration data that allows them to open fraudulent bank accounts and credit cards, acquire mortgages, or apply for other official documents, such as passports and identification cards. Children are targets for this crime: theft of child identities is on the rise in the US, and the increase in identity-related crime in low- and middle-income countries, including those in sub-Saharan Africa, suggests that this trend may spread.[14]

Personal identifiers, such as social security numbers or national identification numbers, enable identity theft. Although such identification data is generally thought to be the most vulnerable to fraud, record numbers or other identification tags created during DBR could function similarly, particularly if these numbers can be used to access services. One recent case underscores the value that fraudsters may see in birth data. Near the end of 2013, an illegal US-based service selling personal data on US citizens hacked into several major public records databases, retrieving social security numbers, birth dates, drivers licence numbers, and other data that could then be used for identity fraud. According to news sources, the service has sold almost 3.1 million

date-of-birth records, at a cost of US$0.50 to US$2.50 each, over the course of its existence.[15] Recent incidences of major bank fraud in Kenya, realised in part through misuse of personal data, underscores the risk in low- and middle-income countries.[16]

## 3.2 Privacy violation

DBR presents the potential for violation of children's and caregivers' right to privacy. Personal data, once networked, is at risk of becoming public. The best available technology and data security practices cannot guarantee that data remains protected. This holds true in the private sector, where major corporations face the risk of hackers accessing customers' personal data, and in the public sector, where a 13-year-old boy recently broke into Argentina's online electoral roll and the linked civil registry data.[17]

Once any data becomes publicly available electronically, children and caregivers lose agency over its use. The type of data often present in birth records – as well as the metadata made available by data collection and transmission via mobile phone and web applications – may include gender, location, health, name, ethnicity, and other potentially identifying information that could be used against children's interests via surveillance, physical location tracking, behaviour-based marketing, or other means.

## 3.3 Persecution based on personal characteristics

Electronic availability of sensitive personal data increases the potential for birth registration data to be leveraged for persecution. In an oft-cited example of civil registry data being used to perpetrate mass atrocities, ethnic identity information recorded on citizens' national identification cards was used during the Rwandan genocide.

DBR heightens the risk that birth registration information may be used against members of certain groups because the digital process allows for greater speed and reach in gathering, analysing, processing, and deploying collected and stored electronic data. Digital storage also makes this data potentially available to malicious actors who may be able to violate electronic databases.

## 3.4 Personal security violation or exploitation

Mobile DBR enabling registration outside of a controlled environment (a hospital or a government office) may present personal security risks for children and families and make them vulnerable to forms of exploitation. Registration agents may not always be trusted to do no harm when they visit families in their homes, particularly in the sensitive period following birth. Families may be illicitly charged for registration services or tricked or extorted into releasing more personal data than required or they are comfortable providing. This data may then be maliciously or irresponsibly used. The threat of such violations is highly context-dependent and should be weighed against the alternative security risk associated with travel to an office or hospital.

## 3.5 Exclusion from the benefits of birth registration

Finally, while DBR makes the benefits of birth registration available to children who may not be able to be registered through traditional processes, it may still exclude some categories of children. Exclusion may happen when caregivers are not able to participate in the electronic process because of the limited geographic or social reach of the implementation, failure of the system to reflect the caregivers' personal beliefs or technical capacity, or other intervening factors wherein no other means to register is available or feasible. Those who are excluded could be comparatively disadvantaged, potentially exacerbating existing inequalities. For example, if mobile phone-based birth registration had limited reach in remote areas already cut off from main registration centres, this would further disadvantage those living in these areas.

# 4. Mitigating risks across the DBR system

The child protection threats described above may each be linked to one or more system-level risks – weaknesses, vulnerabilities, or gaps related to key elements underpinning a DBR system. Identifying and understanding these risks can help to find options for system design and implementation to address them systematically, minimising their potential to cause harm.

When looking at the key elements related to risks across a DBR system, practitioners should consider how fixed the constraints are around each. As discussed below, the operating environment poses the most inflexible constraints, while the nature of stakeholder involvement allows for some mitigation. Information and identity management creates significant opportunities for dealing with risks. These categories should help practitioners to consider where they have the most flexibility to meaningfully reduce risk. Of course, these elements should not be considered in isolation, as the interaction between them will strongly influence the risks in a given context.

These elements are displayed in Figure 3 below.

*FIGURE 3*
KEY ELEMENTS INFLUENCING RISK IN DBR SYSTEMS

## 4.1 Operating environment

The DBR system's operating environment may be difficult for implementing institutions to change, or it may be outside the scope of their intervention entirely. This environment largely sets the rules the engagement.

### System context

The potential for child protection threats to emerge will always be largely based in the system context. Research indicates that several contextual factors should be carefully assessed and considered in all system design and implementation decisions, including whether or not to undertake DBR in a given country.

### Closely assess and monitor the following factors:

- Social context. Religious, ethnic, or other social divides may lead to system design that excludes groups of individuals. Social rifts or even unfamiliarity between implementers and families may be cause for misunderstandings and mistrust. Concerted marginalisation of particular social groups or a history of intergroup violence are warning signs, as improved data on populations could be used to systematise oppression or even social violence.
- Access to key resources. Significant inequalities suggest that there will be widely varying needs among families the system seeks to serve. There is potential for DBR to exacerbate existing inequalities if it cannot meet all the needs of the already marginalised. Unequal access to economic opportunity, infrastructure, education, technology, and other factors may impact a family's ability to benefit from DBR.
- Institutional stability and implementation capacity. For a DBR system to be successful, an implementing government must have the capacity to ensure comprehensive implementation and compliance over time. High political volatility and incidents of political violence also present greater risks.
- Additional context-dependent factors. Additional factors, such as social and cultural norms, negative experiences with mobile banking or other services that are analogous to DBR, or other factors that may influence the level of trust in a DBR system or its implementers may be present in a given DBR context.

Contextual knowledge from existing feasibility studies and previous country work can bolster an actionable understanding of how context may impact risks during implementation.

## Legal framework

The legal framework regulating DBR implementation is critical to providing protections to children and caregivers and ensuring accountability of implementing organisations and participants. Therefore, legal frameworks should form the backbone of agreements made between implementing partners regarding data management, ownership, and sharing. Legal standards include relevant international standards and national and local legislation regarding registration, children's rights, and data protection rights. These typically include civil registration law and other statutes defining and regulating the process of DBR, such as e-security laws, privacy laws, and health sector patient privacy and confidentiality laws, and others.

Assessing the policies, laws, and standards governing DBR, and in particular the protection of personal data, will reveal risks specifically related to digitisation. A well-enforced legal framework supporting children's rights should be the cornerstone of a DBR system.

### Put in place progressive and comprehensive data protection legislation

Countries that are establishing their e-government and digital CRVS programmes may not yet have legislation that adequately protects children's and caregivers' right to privacy and agency over their personal data. In the absence of strong national regulation regarding data security and privacy that specifically addresses digital technologies, there may be discrepancies between national legal protections and vulnerabilities related to technologies.[18]

The prevailing legislative frameworks around data protection are:

1. omnibus data protection regulation in the style of European Union laws regulating the management and use of all personal information
2. US-style sectoral privacy laws that address specific privacy issues arising in certain industries and business sectors, so that only certain types of personal information are regulated
3. the constitutional approach, whereby certain types of personal information are considered private and inviolate from a basic human rights perspective, but no specific privacy regulation is in place otherwise.

Each approach offers benefits, and countries are able to adopt provisions that are most contextually appropriate.

Whatever model it follows, legislation must be comprehensive, precise, and contextually relevant. Analysis of the legal framework should identify any loopholes or conflicts that could weaken the right to informed control of one's personal data. Furthermore, the full suite of policies, laws, and regulations should support robust information governance and identity management schemes (discussed in section 4.3 'Information and identify management' below) at work in DBR implementations and across government activities.

**Looking for stop-gap legislation**

Regulation can help ensure data security even if ownership and usage permissions are not well defined among implementing partners. US health data legislation, for example, includes a 'business associate' clause that makes third parties potentially responsible for conforming to health information privacy statutes if they are performing functions for a health provider or related entity.[19] Applied to DBR regulation, this principle could be used to hold private partners with access to birth data to high privacy standards if omnibus privacy regulations are not in place.

In addition to the codified legal framework, understanding the normative framework governing implementation is important as well. Customs, habits, and accepted practices that make up norms point to whether protections not expressly codified may be followed in practice, or if the statutes that do exist are or can be enforced.[20]

Specific application of data protection regulation is discussed in relation to process steps in the following section. In addition to national-level regulation, industry standards, organisational policy of implementing partners, and agreements between these partners – including MOUs and contracts – should be put in place and harmonised to eliminate system loopholes that could allow harm to children.

## Integration into capacity-building initiatives

The relationship of a DBR system to other governmental capacity-building initiatives will impact its reach and its integration with other key processes and services, and will likely have a bearing on the political will and resources dedicated to it. DBR initiatives that begin as a local project or pilot and grow without systemic support may face increased risk of DBR processes, management, and resourcing being ad hoc.

### Integrate DBR within CRVS strengthening efforts

There is a growing consensus among international child rights, public health, and civil registry professionals that birth registration is most effectively positioned as a fundamental component of a comprehensive civil registration and vital statistics system.

Stating that "improvements in birth registration are rarely possible unless the civil registration system as a whole is improved," UNICEF advises placing a DBR initiative within an overall programme of civil registration and vital statistics (CRVS) strengthening.[21] Such positioning has the potential to streamline DBR implementation, increase interoperability, and reduce the risk of creating

silo-style incompatible processes that increase the risk of data loss, inefficiencies, and prematurely obsolete systems. CRVS upgrades, in turn, should be designed, for example, to incorporate the potential data-sharing processes made possible by DBR.

Looking to a level higher, ideally, both DBR implementation and CRVS strengthening initiatives would also be designed and implemented according to an overarching national ICT strategy or other broad e-government initiatives.[22]

Even when starting with a small pilot, the design and implementation of DBR initiatives should prioritise integration with such larger initiatives.[23] Such integration may be difficult to manage in practice, but it is necessary to fully realise the benefits of DBR.

## 4.2 Stakeholders

Stakeholders are the organisations and individuals who are involved with and impacted by a DBR implementation. Their constraints, needs, and interests will drive decisions shaping the system.

### Institutions, agencies, and organisations

Stakeholder institutions, agencies and organisations include implementing partners and data recipients.

Implementing partners: Implementing partners include the bodies that act as registration facilitators and supporting organisations. Typically, DBR is undertaken by a government agency and may have the support of international partners, including international financial institutions and other donors, international development and/or child rights organisations, local partners, technology partners, and others. This collaboration can provide enormous benefits, such as access to technical and implementation expertise, but it also carries with it programmatic risk. Risks arise when these partners are not aligned in mission, values, and expectations, are poorly coordinated, and agreements governing their partnership are inadequately defined.

Data recipients: Data recipients are defined by the legal framework and may be government agencies, or public and private organisations that have the ability to receive and use data created and stored during DBR implementation. While generally not heavily involved in DBR system design and processes, these stakeholders have the potential to misuse system data.

The following steps may help identify and defuse specific risk factors relating to institutions and organisations.

## Assess the interests, capabilities, and motivations of the implementing partner organisations

The interests, capabilities, and motivations of partners will reveal issues that should be addressed in system design and implementation.

Third-party partners and technology providers should be thoroughly vetted, both for trustworthiness and fit. Anecdotal evidence suggests that some third parties have taken personal data, either in breach or in absence of strong ownership agreements.[24] Because commercialisation and misuse of personal data are key risks, third-party partners should be avoided if they have a history of allowing data breaches, failing to sign or honour strict data protection protocols, or enabling privacy violations or exploitation of any kind of their products' end-users.[25]

Institutional bodies should be assessed as well. Do the lead and supporting implementing agencies have the necessary financial, human and technological resources to carry out DBR according to acceptable standards? Agencies that are able to build and manage technology and data themselves may minimise risk by keeping these processes centralised and more easily monitored and controlled.

Top-notch advisers and subject experts are important partners, but are only as effective as their ability to connect with members of implementing agencies and work in context. Implementing agencies should seek out technology and data security advice from relevant experts where necessary to support alignment between technical expertise and humanitarian interests.[26] Child protection organisations can play a key role in connecting governments to relevant expertise, supporting the inclusion of child protection in a DBR implementation.

## Codify partner expectations, roles, responsibilities, and accountability checks

There is opportunity for partners to be misaligned on the goals, standards and processes for DBR. For example, partners may adhere to different standards of what constitutes serious child protection risk and privacy protection. Formal and binding agreements should leave no room for misalignment on these important points.

These agreements should go hand-in-hand with the prevailing legal framework, and may plug holes in regulation.

## Centralise management authority

UNICEF recommends establishing a monitoring body, led by the Ministry of Health and Civil Registration authority, to oversee management of the system and its implementation, provide quality assurance, and promote integration with other agencies and processes.[27] Within the context of CRVS system strengthening, this monitoring body is likely to be the CRVS Steering Committee. This body can help ensure cooperation in implementation and uniformity of standards across jurisdictions – a challenge for DBR, which often capitalises on the benefits of decentralising the birth registration process.

## Ensure effective coordination and communication between partners

To ensure that partners collaborate effectively at the process level, coordination and communication strategies should be well developed at the system level.

Poor information-sharing between partners can exacerbate weaknesses in partnership agreements or differences in perspectives and lead to system failures. In one instance, an organisation launched a pilot DBR initiative with volunteers as registration agents, only to find that local government officials disapproved.[28]

It is important that DBR implementers define information-sharing needs to institute clear communication and coordination protocols. A child protection organisation is often in a prime position to coordinate this process, as they may be the link between the implementing government, technology providers, and third-party partners.

## Manage data recipients according to their interests, capacities, and roles in DBR

As with implementing partners, the interests and capacities of data recipients should be assessed for their potential to increase risks. This assessment can be applied to agreements and activities of the implementing partners (e.g., agreeing to institute strict controls on data-sharing with third parties if there is a high level of interest and ability among these parties to use birth data for targeted marketing). Where appropriate, data recipients should also be engaged as allies to both counteract risk and increase benefits of DBR. For example, government agencies that can better support children's welfare with streamlined access to birth data should be involved, given they can meet capacity requirements. Such involvement should be continually managed by the lead DBR implementing agency.

## Individual participants

The individuals involved in a DBR implementation include the staff and volunteers in partner organisations (from registration agents to civil servants to technologists), as well as the families (caregivers, parents and children) who are meant to benefit from DBR. The success of a DBR initiative depends on how well it incorporates and responds to the interests, capabilities, and motivations of these participants.

For architects of a DBR initiative, therefore, it is important not only to identify the system's participants, but also to understand them in the system's implementing context. Assessment of the following factors can point to accountability mechanisms, training, and incentives to provide for implementers, on the one hand, and the information and support families need to exercise their right to identity, privacy, and agency over personal data on the other hand.

### Understand the value of registration and the data created during DBR to different participants

The outputs and outcomes of DBR – namely, birth data and registration leading to an official identity – will mean different things to different participants. They may represent access to education and other essential services, a regular wage, a bureaucratic hurdle, or potentially an opportunity for high profits through fraudulent activity. Understanding the value that DBR creates for those involved can point to the potential for abuse as well as programmatic opportunities.

### Assess participants' abilities to access and use technology underpinning the programme

Technological abilities of DBR implementers may introduce risks related to their involvement, from potential user errors and oversights stemming from low abilities, to abuses of the system by those with superior technology skills. Technological literacy and access may influence families' understanding of DBR, their understanding of the risks involved, and their ability to participate fully in different stages of the programme. Other factors to consider when assessing and developing mitigations for these risks include environmental and economic barriers to technology use among all segments of participants.

### Analyse potential unauthorised participants

Finally, architects of a DBR system should perform this same analysis on those who would participate illicitly. While technically outside the DBR system, these illicit participants may have a significant impact on the system. Risks and mitigations related to these actors are primarily discussed at the process level, but their interests and capabilities should also be a factor in system design.

## 4.3 Information and identity management

DBR requires effective management of personal information and identity, two of the most valuable assets related to birth registration. By increasing the ability to share information across a greater number of channels, DBR requires governments to institute more sophisticated information management schemes than were previously in place. The ability to authenticate or verify an individual's identity is critical to ensuring that only authorised participants are able to access the information related to DBR, and that these participants are accountable for managing this information appropriately.

Vulnerabilities in information and identity management schemes can allow both malicious misuse and innocent mistakes that lead to harm for children. Putting in place stringent protocols, leveraging the best available technology, and maintaining multiple levels of human oversight are key measures to minimise the risk of such harm occurring.

### Information governance

Data, and its processed and applied counterpart, information, are key inputs and outputs of DBR. An information governance framework sets the ground rules for information that will be handled across the programme, defining the authority and decision-making structures regarding data and information across the administration of a DBR programme.

#### Implement a robust system-wide information governance framework

DBR implementations need a clear information governance framework articulating the mission, roles, responsibilities, protocols, and processes around the management of data and information created and shared through the system. Like the legal framework and partner agreements shaping system implementation, a good information governance structure should clearly articulate these components and leave as little as possible to interpretation. This framework should flow from the overall project architecture, and respond to the project context.

The information governance framework should establish standards, practices, and tools of data management that can be implemented across the system. Key aspects of data management that should be covered in the framework include:

- quality control (auditing to ensuring the accuracy, completeness, and validity of data)
- data minimisation (limiting data to the most necessary elements needed for the desired objective)

- appropriate security measures (that are equal to the sensitivity and value of the information contained in the system). The international standard of IT system security (ISO27001) should provide a common point of reference on this point. It provides requirements for establishing, implementing, maintaining and continually improving an information security management system
- authorisations and exclusions (measures to keep unauthorised users out of the system).

The technology and procedures outlined in the framework should also be sustainable in context and appropriate to the financial, human, and infrastructural capacity of the implementing environment.

Specific tools and protocols will vary (and are discussed in regards to DBR processes in the section that follows), but a strong public key infrastructure is advantageous, if available. However, to be effective, it requires that participants have already proven their identities and right to access the system.[29]

## Identity management

To effectively implement protocols defining who has authority to control data and information, it must be possible to verify the identities of participants. Verification depends in large part on the overall identity management scheme present in the implementing jurisdiction, and therefore proves challenging in environments where general identification systems are weak (e.g., in the absence of national ID systems).

### Establish multiple layers of identity verification across the programme

All DBR participants – health practitioners, registration agents, parents/caregivers, and third parties managing and receiving data – should ideally have their identities verified in order to participate.

Identity verification is generally based on at least one of the following: 1) something the individual in question has, such as an ID card; 2) something that person knows, such as a password; 3) something that person physically possesses, such as fingerprints or other biometric tags.[30]

Different forms of identity verification will be applicable for different actors and at different stages of the DBR process. However, they should all rely on a combination of an advanced electronic signature scheme and manual checks.

Even in the absence of comprehensive identity management systems, DBR can leverage what systems exist. Professional digital identity management systems for health providers can build on civil identity, for example, by using existing staff identity authentication protocols to ensure that only authorised hospital staff are able to submit their designated portions of birth registration documents.

The implementation of a DBR system may also provide impetus for improving identity management capabilities across agencies by creating a platform for advocating for and modelling overall identity management schemes.

### Registration, identification, and identity verification

Because birth registration does not in and of itself create a formal proof of identity, robust data protections and identity verification may seem most relevant to impose during the identification phase following registration. However, linking registration to identification with fewer inefficiencies and barriers is one of the key advantages that DBR offers. Creating this streamlined and integrated process (as in Uruguay, for example) calls for protections appropriate to identification to be included throughout the birth registration process.

As with other cornerstones of DBR, information governance and identity management should not be considered measures that can run on autopilot. Purposeful redundancy is key – multiple checks should be put in place at each level so that, for example, it is never possible for just one person to approve registration or distribution of birth data.[31] These frameworks should be continually assessed, refined, upgraded, and supplemented.

# 5. Mitigating risks in each step of the DBR process

This section builds on the discussion in the previous section of how DBR-related risks may be considered and addressed at the system level. It details how specific risks may arise at each step of a DBR process, and presents practices to mitigate them.

## Model birth registration process

Figure 4 layers prominent risks related to each step of DBR on the process map introduced in Section 2. The pages that follow discuss these risks and corresponding mitigation strategies in greater detail.

*FIGURE 4*

DIGITAL BIRTH REGISTRATION FLOW

## Step 1.
## Notification and birth data collection

To start the registration process, the parent, caregiver, or health worker informs the registration agent that a child has been born. The registration agent then collects the necessary data from the parent or caregiver to initiate the creation of a birth record. In a hospital or institutional setting, the data is likely entered into a desktop computer. When collected within the community, the data may be entered into a mobile phone, a tablet, or, less frequently, a laptop.

### Risks

#### 1. Unauthorised access to registration system via data collection device.

As numerous examples from the government and corporate sectors have shown, lost or stolen mobile phones, laptops, and other devices can provide access to stored or submitted data. Unauthorised access can occur even while the authorised agent possesses the device: bluetooth-enabled mobile devices, for example, are particularly vulnerable to being hacked.[32] Further, if registration agents are able to use their own phones, agent and system beneficiary data may mix.

#### 2. Data is recorded incorrectly, creating an erroneous record.

Poor user interface design or poor agent management can contribute to erroneous data submissions, which can be difficult to detect and even more difficult for a caregiver to correct.

#### 3. Caregivers provide personal data without understanding its uses.

Parents and caregivers, especially those who are unfamiliar with technology, may be unaware of what information is being collected, how it will be used, how it could harm them and their child as a result, and what recourse they have. Registration agents may not be under any obligation to provide this information or may not have it themselves.

#### 4. Inflexible systems or other failures may exclude children from registration.

Highly automated processes and requirements may exclude children of parents/caregivers who are unable to present standard identification documentation and parental authentication. Children living in low infrastructure regions or outside the areas of outreach efforts may be excluded from both analogue and digital processes. Similarly, legacy records from analogue systems may not transfer easily, leading to the exclusion of children whose records are never reformatted and integrated into the DBR system.[33]

### 5. Families are subjected to exploitation or other harm by registration agents.

Greater decentralisation may create greater opportunity for children and caregivers to be victimised by those facilitating the registration process. In Ghana, registration agents have been found to illicitly charge families a 'fee' for a registration process that is officially free.[34] In remote communities, imposter registration agents could similarly exploit parents. Inviting registration agents into the home puts families at risk of theft or physical assault. Such negative experiences, in addition to the immediate harm they cause, may dissuade some families and exclude others from the process.

## Mitigations

### 1. Secure devices with strong technology and management protocols.

Devices and data should be password- or PIN-protected via the phone's or computer's software. Regular data wipes should ensure that little data is stored outside the registrar's database.

Allowing registration agents to use their own devices to collect data may be initially cost-effective and beneficial, but this sharply reduces DBR implementers' control over device and data use. Information sent via personal devices should be strictly limited and software should include appropriate access controls.

### 2. Ensure registration agents have necessary capacity and are accountable.

DBR systems employ a variety of community health workers, civil registry staff, and others to collect data. All agents should receive a level of training appropriate to their role, including information about child protection threats and guidance to appropriately express these risks to caregivers. Making training accessible and relevant may include training in interview and research techniques and ethics, creating glossaries, and recreating information reporting formats so that they are user-friendly.[35]

Registration agents should also be closely managed. This could include checks on their data, automated proof of correct execution, periodic shadowing by supervisors, and community accountability structures.

### 3. Prevent potential abuses in later stages by limiting data collected.

The practice of minimising data made available should be incorporated in system-wide standards, but it is especially important at the initial collection phase. Particularly if strong data protection measures and sharing mechanisms are yet to be put in place, data collected should be restricted to the minimum data needed to facilitate registration. The latest recommendation from UNICEF is that these minimum pieces of data are: child's name at birth, child's sex, child's date and place of birth, parents' names and addresses, and parents' citizenship.[36]

It is important to note, however, that effectively minimising data requires analysis of the sensitivity of different data; choosing to collect four pieces of high-value data rather than 20 pieces of low-value data is not logical data minimisation.[37] Calculation of what constitutes appropriate data minimisation given the goals of DBR requires contextual analysis.

### 4. Institute context-appropriate informed consent practices.

Data collection provides a crucial in-person opportunity for informing caregivers and parents of their rights regarding personal data, helping ensure that the data processing that follows has a basis in real consent. Consent should be freely given, explicitly confirm the individual's wishes, and be documented for verification.[38]

DBR systems should make obtaining and documenting informed consent a mandatory part of the data collection process and consider ways to accurately convey DBR-related risks in a context-appropriate way. Given the paper-based birth declaration forms currently used, obtaining formal consent at the point of data collection will not differ greatly from many existing processes. Analysis of humanitarian, public health, and mobile cash transfer programmes shows a consensus that the following information should be conveyed as the basis for consent: i) the nature of the data being collected; ii) the organisations and agencies that will have access to the data; iii) the body that is charged with ensuring the data is kept secure; iv) information on how to contact this body and access/change the data; and v) recourse to recall their data, withdraw consent, or otherwise limit access to the data after the fact.[39]

Practitioners should seek to identify barriers to informed consent in a given context – whether that be lack of knowledge about the technological risk, reticence to ask someone acting in an official capacity for explanation or additional information, or an eagerness to have their child registered that supersedes concern about the risks (known or unknown).

To ensure that consent is truly informed, practitioners should develop ways to translate this information and other complex concepts central to DBR and data privacy into language that will resonate with local populations. Visuals tailored to the specific audience may be helpful in this regard. Visuals created to help explain data privacy regulations and creative commons rules provide examples of such materials.[40]

It is worth noting that consent may be somewhat questionable if caregivers do not find the available data protections adequate but still want to register their child. Following the principles of right to control of personal data and data minimisation, it may be feasible and desirable to include an opt-in option for collection of data not critical for registration, or to include provisions allowing caregivers to stipulate that data may not be used for behaviour-based

advertising.[41] At minimum, parents and caregivers should receive information detailing how they may express their opposition to the process if they wish, and an official process should be put in place to address such feedback.

### 5. Include alternatives for those who are excluded by the digital process.

Maintaining options for manual registration – as well as information access later on in the process – can help prevent disenfranchisement. Matching registration requirements to parents' available means of identity documentation and making different combinations of means of verification acceptable can help reduce exclusion in the first place. Appropriately targeted outreach efforts can help close gaps in coverage by providing information to caregivers and uncovering other potential barriers to participation. Outreach efforts that have been previously led by members of communities who are less knowledgeable about the technology involved may need to be adapted.

## Step 2.
## Birth data submission to registry database

The registration agent submits the necessary data to the registrar using the system's protocol and tools. To complete the submission, the agent verifies his/her own identity to the registrar. In some systems, this may occur automatically if the agent submits information via a mobile phone with a registered SIM card or via a secure web form. This data is then logged in the database to be reviewed, verified, and processed. An initial birth record may be created at this stage. The parent or caregiver may also be given a receipt at this stage, for example an SMS or email message with a temporary registration/identification number.

### Risks

#### 1. Birth data sent or preliminary confirmation received is exposed to unauthorised parties.

For outsiders to the DBR system, gaining access to stored text messages is challenging but not impossible, as intercepting software can be used by third parties.[42] Network operators are also often obligated to store data for a certain length of time, increasing the risk that data could be seized after transmission.[43]

Registration agents using their own or unregulated phones could potentially send collected data directly to outside parties. The registration authority may have limited licence or capability to monitor personal phone use among registration agents. Interception could also occur when a preliminary registration confirmation message is conveyed to the caregiver via mobile phone, an email account, or other digital means. If the caregiver's phone, email, or computer is shared among multiple people, those people could also gain access.

#### 2. Metadata collected during notification is made available to third parties or other unauthorised users.

Mobile phone user records on operator servers include private information such as calling activities, user location, and billing information. Though this information is mainly handled by the operator, outsider access to user records should not be excluded as a possible risk.

#### 3. Fraudulent data is submitted.

As with lax in-person processes, authorised and unauthorised users alike may theoretically submit false registrations or distort data if appropriate technological and management identification and prevention measures are lacking.

## Mitigations

### 1. Include security measures in preliminary registration confirmations.

Caregivers may be required to create a personalised digital account to be able to receive registration confirmation. Alternatively, they may be asked to enter a self-chosen password during data collection in order to receive their confirmation.

### 2. Encrypt data at all possible points.

Software used for DBR should automatically encrypt information sent via mobile networks or web connections, though the type and strength of encryption may vary. Implementers should always consult technical experts to ensure that the highest appropriate standard of encryption is employed during data transmission. Encryption provides critical access control across the DBR system, and so additional opportunities for encryption, such as when data is being stored in the database and on collection devices, should be used as well.

### 3. Implement strict transmission permissions.

In addition to the device access protections mentioned above, DBR system software should include features preventing fraudulent submissions or illicit sharing of data. Dedicated phones can also be programmed to send and/or receive messages only to and from authorised numbers.

The identity of the registration agent or notifier should also be firmly established. There are several ways to do this. In Uganda, for example, registration agents are given SIM cards mapped to their name. In Senegal, chiefs involved in birth registration are given specific mobile phones. Local government registrars reporting births from specific registration centres and in community settings aligned to broader civil registration and vital statistics (CRVS) responsibilities may receive a unique ID. This is the case with the use of RapidSMS in monitoring the reporting frequency of registered births in Nigeria.[44]

However, there still exists the potential for an unauthorised person to use a lost or stolen phone to initiate false registrations if password protection and other security layers are bypassed. An additional layer of protection is required.

### 4. Conclude strong agreements with network operators.

Arrangements with network operators should include agreements that operators will not sell, store, de-encrypt, or use any messages and data sent via their networks. DBR implementing organisations should ensure

that network operators are using appropriately advanced security measures, including mitigating against potential insider misconduct, to keep user data private. However, there are no ironclad guarantees that operators' databases are inviolable or that operators will not have to release user data to authorities if requested.

### SIM-based identity verification

At least 80 countries worldwide (including 37 in Africa) require individuals purchasing prepaid SIM cards to verify their identity and register the SIM in their real name. This represents at least four billion SIM connections.[45] While increasingly popular, the net impact of mandatory SIM registration is debated, and some countries (notably Mexico) have reversed course and removed this requirement.

In a DBR implementation, mandatory SIM registration may provide an extra measure of identity verification for those collecting birth record data. However, there are some important weaknesses of SIM-based identity verification. Without other device-level verification mechanisms, such as PINs or passwords, SIM-based identity verification will not prevent unauthorised users from submitting data if the device is lost or stolen. Countries that require SIM registration have also found there are now black markets for registered SIMs, reducing their reliability as identity verifiers. Requiring SIM registration may also create logistical difficulties or heighten the potential for surveillance and privacy violations to affect DBR participants.

The system environment should be scrutinised to determine the relative advantage of relying on registration agents' SIMs for identification purposes.

## Step 3.
# Data validation and record storage

Upon review of the data and registration agent credentials, the registrar either validates and finalises the registration, or follows up for clarification and/or further documentation. The registration agent or registrar may return – in some cases personally – to the parent or caregiver to address any data discrepancies and validate the registration. When the official birth record is created, the certificate is printed or prepared for printing and picked up at a later time.

## Risks

### 1. Records are intentionally compromised.

Malicious users – either unauthorised users or authorised individuals using access for illegitimate purposes – may take advantage of system vulnerabilities to capture and/or alter data. Such breaches typically get the most publicity when they affect private sector data holders, but public agencies are also targets. There have been cases of developing countries' elections and other databases being hacked or breached for a variety of reasons.[46]

Data storage systems can be compromised when denial of service attacks keep authorised users out of the system. Viruses and worms can infect the database, or the system can shut down due to low technical capacity or other weaknesses.

Cloud-based storage, an increasingly popular option for the many benefits it offers, may also increase the risk of data breaches. Cloud storage may decrease direct control over operations and decisions regarding the computing environment, particularly if it is offshore (though national laws vary on this point).[47]

### 2. Records are lost or compromised due to mismanagement.

While DBR generally has been found to reduce the rate of data entry errors, lack of attention to data quality can introduce or perpetuate inaccuracies, which can be difficult for beneficiaries to correct.[48] Poorly defined or ignored security policies can lead to lax oversight and make data more easily available to malicious misuse.[49] Unavoidable natural disasters and volatile conflict situations may also lead to data loss.

### 3. New data is incompatible or not integrated with existing data.

DBR data may be incompatible with existing data. Files may need to be merged, and old files may need to be validated and entered into the new system. Existing office equipment may not be advanced enough to effectively handle new formats and programs. Previous works by Plan and UNICEF have found that this frustrates staff and increases workload. This decreases the likelihood that staff will use the system effectively and may contribute to a greater error rate.[50]

## Mitigations

### 1. Choose data storage systems with security concerns and institutional context in mind.

The type of data storage system used should reflect the needs of the context, such as the technical capacity of the staff maintaining the system, the local physical and network security system, and the data-sharing protocols in place. Many developing countries use off-the-shelf database software and, while this software may be well known, it may be geared toward developed-country contexts and not easily customizable to specific needs.[51] In contrast to such proprietary software, open source software, whose source code can be freely modified, allows agencies to customize software to their security needs.[52]

Cloud storage can be public (where services and infrastructure are provided off-site over the internet and owned by an organisation selling cloud services), private (where the services and infrastructure are maintained on a private network), or a hybrid of the two (where the mix of public and private elements is optimised to suit the organisation's requirements). A variant of the hybrid solution is a 'community cloud', where infrastructure is shared by several organisations and supports a specific community with shared concerns (e.g., mission, security requirements, policy, and compliance considerations).[53] To address potential risks, DBR implementers should have a service-level agreement that maintains legal protections for privacy relating to data stored on the cloud provider's systems. Organisations must also ensure appropriate integration of cloud computing services within their own systems to manage security and privacy.

### 2. Tightly control access and monitor activity.

Controlling access to databases requires a combination of technology solutions and management protocols. To minimise potential for data misuse, staff access privileges should be limited to the lowest level necessary for a staff member to perform his or her job. This can be achieved by tightly defining user profiles and corresponding privileges for viewing and processing data. It may also be useful to compartmentalise data so that more sensitive data is subject to stronger protections no matter who is viewing it.

Intrusion prevention systems can be designed to match access restrictions, even if they are not considered fail-safe. Strong authentication protocols matching levels of access are critical to keeping unauthorised users out of the system. This requires a technical solution – such as two-factor, or two-step, authentication – as well as communication and maintenance of strict username and password policies among users.

In addition to controlling data access, network-auditing programs can catch irregularities, reveal breaches, and help ensure accountability. Intrusion prevention systems can also identify patterns linked to known system vulnerabilities and track suspicious or threatening use for further investigation.

Finally, prudent security mechanisms and protocols limiting physical access to data storage devices still need to be in place and complied with, no matter how advanced the technological protections are. Such protocols include keeping devices in locked, limited-access rooms when not in use, as well as rules and checks to keep staff from taking office equipment and records out of the office.

### 3. Include quality assurance mechanisms with a manual or human component.

Data should be regularly checked and corrected using a combination of manual and automatic processes to ensure accuracy and completeness. The US state of Oregon, for example, is recognised for its support of health institution staff in submitting clean birth data. In Oregon, designated birth clerks responsible for sending birth data to the state registry are also responsible for correcting their own errors. The state registry generates an automatic error report for each clerk that is securely emailed to him/her every two weeks. The birth clerk is then required to correct the errors and resubmit a corrected report, creating an accountability loop. Oregon registry staff found a resulting increase in the rate of error correction.[54]

Quality assurance must continue after initial validation: managing data over its lifetime is critical. Birth records can be linked to additional and updated identifiers for verification purposes – from photos to biometric data – to decrease the likelihood of identity fraud.[55]

### 4. Promote human capacity to pre-empt violations.

Security measures should be enforced by capable and accountable database administration staff following agreed-upon protocols to monitor the system. They will need to be educated on relevant risks and have access to frequent training sessions and awareness activities built on appropriate messaging. Clear policy on data permissions and accountability measures should be communicated to all those involved.

### 5. Build necessary capacity for technical upgrades into the system design and budget.

Staff cannot be expected to shoulder the burden alone. Building customized software to integrate old and new systems is one creative solution. The need for ensuring that DBR systems are integrated smoothly with existing data and practice to the extent possible argues in favour of incorporating DBR implementation with CRVS upgrades to capitalise on economies of scale and decrease disruption.

### 6. Enable effective data recovery through planning and appropriate technology.

Understanding the requirements (in terms of time, people, and equipment) needed to recover data and get the system back up and running can help the central authority and local registration offices plan how to react in cases of data loss or system outage.

To prevent data loss, the implementing agency should maintain a local back-up source, rather than only a remote one, especially for data that needs to be recovered frequently. For a local back-up to be an effective option, the back-up servers should be in a location that is available around the clock, able to be quickly transported back to the relevant office or data centre, and able to be securely accessed by more than one employee. Back-up data should be encrypted as well.

One person should hold responsibility for designing all back-up and recovery processes, regularly testing them and keeping them up to date.[56]

## STEP 4.
## Birth record data is shared and distributed

Birth record data may be shared with additional agencies, and potentially other third parties, according to the agreements in place. This step may or may not take place, depending on the implementing context and agreements between implementing partners and other bodies. When birth record data are shared, it may be done through formal requests between agency personnel or queries via web interfaces. In some instances, data may be shared automatically. Greater interoperability is one of the key benefits offered by DBR, but may also exacerbate system vulnerabilities.

### Risks

#### 1. Data and databases are compromised during sharing.

While similar to access-related risks in other stages of the registration process, sharing of data by authorised data users via devices and channels geared toward general consumer use poses a particular risk. Official and personal files may be mixed, and new forms of viruses or other malicious software (malware) may be introduced.

If birth registration is tied to other social benefits and digital systems are integrated, there exists potential that a more secure system will be accessed and compromised through a weaker one. Hackers or fraud perpetrators may target birth registration data shared directly between agencies because of the possibility of a resulting link to public systems distributing social support payments. Conversely, a relatively secure birth registration database may be compromised if it is linked to a less secure database managed by another agency.

#### 2. Shared data is commercialised or used irresponsibly by receiving parties.

Partnerships with commercial partners, especially those in the field of digital technology, can provide resources and expertise to promote the success of DBR initiatives. However, these partners may secure the data with less care and have an incentive to use collected data for their own interests, such as for targeted advertising.[57] This currently happens when data aggregators comb public records, including birth records, copying personal data and selling them to advertisers and marketers hoping to micro-target consumers online.[58] This practice may not be directly relevant for countries where DBR is being newly implemented, but concerns around commercialised data – especially via cheap mobile services – will likely become increasingly serious.[59]

#### 3. Children and caregivers have no agency over how their data is used.

In the absence of strong regulation, these key users may not be able to know or influence how their data is shared and may not be informed of database breaches.

## Mitigations

### 1. Codify and enforce strong privacy regulations.

Regulations governing data sharing can provide directives and accountability measures that promote secure use of personal devices and publicly accessible platforms. At minimum, such regulations should include provisions governing the scope of coverage, consent and notifications, data storage and accessibility, and cross-border sharing and third-party transfer restrictions.

### 2. Process data before sharing to minimise exposure.

Data should be anonymised so that it cannot be matched to individuals. According to the needs of data recipients, data may be aggregated, masked, or shared in a derived format.[60] When considering how much data to share and in what format, children's security should be given first priority over the needs of third parties or partners.

### 3. Strong agreements with shared agencies and partners over ownership, licensing, and sharing permissions.

Agreements between implementing partners should be precisely constructed so that they take advantage of data ownership and legitimate use provisions laid out in national regulations. Where such regulations do not exist, agreements should attempt to include their protective measures in the terms of the agreement. Contracts with partners, especially third parties, technology providers, and network operators should be structured carefully to ensure that data ownership is clearly defined and is in line with such regulations.[61] Where cross-border partnerships exist, all other things being equal, implementing organisations should seek to have contracts governed by the applicable jurisdiction that offers the strongest child and/or data protection measures.[62]

### 4. Share via enterprise-scale platforms, software, and devices.

Cloud computing allows governments to more easily utilise affordable commodity ICT products and services.[63] When seeking secure platforms for storing and sharing data, governments may opt to create an internal, private cloud when a publicly available cloud platform does not provide a high enough level of security for sensitive data.

## Step 5.
## Data is queried, checked, and corrected

Individuals have the right to request, view, and correct their personal data. Depending on the openness of the system, individuals may have access to data of varying sensitivity when querying one record. Through DBR, individuals may be given the ability to view and correct their own information or that of their child online or via other electronic means. In more open systems, individuals may be able to query data belonging to others as well.

### Risks

#### 1. Caregivers are unable to access and correct records, excluding children from benefits.

Digital modes of record querying may exclude vulnerable populations whom DBR is intended to benefit by requiring some form of network access and appropriate devices.

#### 2. Unauthorised users access and/or alter birth data.

Unregulated systems may make selected birth data available to a potentially vast array of actors. The consequences of this depend on the laxity of the system, the mode of access, and the data displayed and linked to the record. So-called 'open records' states in the US, which make birth records available upon request to anyone who asks, have seen a dramatic jump in requests in recent years. There is evidence that this increase in requests is linked to the corresponding rise in identity-related crimes.[64] (These states, however, do not allow records to be altered through such unregulated processes.) This has raised real concerns about the rise in identity fraud that could be directly linked to this poorly restricted access.

### Mitigations

#### 1. Make analogue processes available alongside digital.

Moving birth record look-ups and data delivery completely to the electronic world may make the data inaccessible to users who lack the necessary technological resources or knowledge. To the extent appropriate given particular local needs and feasibility, DBR implementers should make analogue data delivery and assistance options available. Mandates enforcing the right to access and correct one's own data may specify modes of access and processing timelines for change requests to support look-up and modification options available to all legitimate users.

### 2. Create strong authentication processes for users accessing data.

Similar to security measures necessary for sharing of birth record data among other agencies and third party partners, identity verification and proof of authorisation to access data should be required of individuals seeking to view and potentially alter birth record data. Multi-step processes that include both automatic and manual identity verifications make the strongest stand against illegitimate access.[65] For example, state- or province-level birth record look-up services may involve human checks that planned data use will be legitimate. This may include manual review of submitted copies of identification documents, as well as data-seekers' rationale for accessing the data.

### 3. Match data display and delivery details to risk potential.

DBR system design should consider the legitimate uses that those with rights to view and update the data might have, and limit electronic delivery of that data to the minimum necessary to accomplish those goals. This may involve making data available in waves – for example, linking the name to a record available with a lower level of user authentication, and delivering more sensitive data, such as a linked birth date, address, and national identity available for users who undergo more thorough identity validation.

ERIK THALLAUG/PLAN INTERNATIONAL

# 6. Closing thoughts

The application of a new technology to an old practice always raises exciting possibilities. With the digitisation of birth registration, the potential for expanding reach of government services means extending the social contract to those who would have previously been excluded. As experience demonstrates the real-world benefits of DBR, implementers must continue to proactively mitigate the potential risks that may accompany them.

Doing so requires a holistic approach and adaptability. A DBR system is shaped by its economic, political, and social context. Though this document has divided risks into discrete categories and matched them to specific mitigations for clarity, in real-world implementations, risks are likely to have complex origins. For example, although the proximate cause of data entry errors may be poor software design, the poor design may be rooted in miscommunication between technology advisers and DBR system designers, pre-existing agreements with software providers, and insufficient staff training. To be successful, mitigations must address these combinations of underlying causes, rather than just the symptoms.

Continual iteration is also needed to maintain systems. Implementing partners must be able to anticipate how technology use may change in the years ahead and effectively foresee potential failures and abuses that may emerge. To this end, implementing agencies, as well as involved child protection advocates, should engage deeply with technologists and build technical capacity in-house.[66] This will make it possible to assess the full scope of technological capabilities from a child protection and civil registration perspective.

Finally, implementing agencies bear the responsibility of mitigating risks in relation to potential benefits. Determining the proper balance between risk and benefit is a question that should be extended to those at the heart of the practice: parents and caregivers, children, and citizens whose identities will be incorporated into the system. DBR implementations should involve communities at each stage to ensure the designs meet the demands of the most important users. To this end, awareness campaigns and co-design processes (not discussed in this document) should be an integral consideration. Citizen feedback and social accountability are the ultimate risk mitigation strategies.

ERIK THALLAUG/PLAN INTERNATIONAL

# 7. DBR risk assessment tool

7.1 User guide

7.2 List of risks and mitigations for each step in the DBR process

## 7.1 User guide

Digital technologies have the potential to expand the reach and benefits of birth registration. However, digitisation also brings child protection risks.

This tool helps you understand and address those risks. The tool provides:

1. checklists of likely risk factors
2. example risk mitigation mechanisms for each
3. prompts to develop context-based responses.

The significance of risks depends on the digital birth registration (DBR) system's context and design. Consider the risks and mitigations described in this tool together with other assessment and evaluation mechanisms. Adapt this tool to fit your needs.

### Who should use this tool

Plan staff and/or other assessors should complete this tool. It can be completed by an individual or a group, e.g., in a workshop setting.

### How to use this tool

The tool is split into stages based on when you are engaging with a DBR effort.

| WHEN YOU ARE... | USE WORKSHEET TABS... | TO IDENTIFY RISKS AND MITIGATIONS FOCUSED ON.... |
|---|---|---|
| Preparing to engage in a new or ongoing DBR effort | A. Before engagement | Broader context and general stakeholders |
| Designing a DBR system or assessing a proposed design | A. Before engagement<br>B. During system design | System design, implementing partners, data management, and technology |
| Evaluating an ongoing DBR system implementation | A. Before engagement<br>B. During system design<br>C. After implementation | Actual practices and realised threats |

### How to complete each section

1. **Complete the questionnaire.** Answer all questions in the 'Risk factor' column, recording the answer as 'yes', 'no', or 'unclear' for each. Provide any relevant additional information in the 'Detail' column.
2. **Assess risks.** Questions that received a 'no' or 'unclear' answer are risk factors in your context. The 'Significant risks' box near the bottom of the section provides space for summarising these risks.
3. **Identify existing mitigation measures.** Record mitigation mechanisms currently in place in the 'Existing mitigations' box near the bottom of the section.
4. **Plan future mitigation measures.** Assess gaps between relevant risks and the mitigations currently in place. The 'Mitigations to consider' column provides examples for each risk. Use these to plan for new mitigations in the 'Further mitigations' box at the bottom of the section.

## For more information

This tool accompanies the report *Mitigating Risks to Children in Digital Birth Registration Systems*, available through Plan International. The report describes the risks and mitigation mechanisms presented in this tool in detail.

# A. Before engagement

This section covers risks related to a DBR system's context and stakeholders. Always complete this section before moving on to the 'During system design' and 'After implementation' tabs. For each risk question below, answer yes/no/unclear and add details. Then, summarise the risks, existing mitigations, and planned future mitigations at the bottom.

| | RISK ASSESSMENT QUESTIONS | YES/NO/ UNCLEAR | DETAIL | MITIGATIONS TO CONSIDER IF 'NO' OR 'UNSURE' |
|---|---|---|---|---|
| OPERATING ENVIRONMENT | | | | |
| **Political and governance context** | | | | |
| This includes the governance, social, economic, and technological context surrounding a DBR system. These contextual factors can contribute to exclusion of or harm to some families through DBR implementation. | | | | |
| 1 | Are the minority or marginalised groups protected from persecution and oppression? | | | Consider underlying causes of these risks, and the possibility of addressing them sustainably through DBR system design. If risks are significant and cannot be reliably mitigated, advise against pursuing DBR at this time. |
| 2 | Are key resources – e.g., technology, education, wealth, fairly evenly distributed throughout the system context, with no severe cultural, regional, or other disparities? | | | |
| 3 | Have existing e-government programs managed user data responsibly and protected user privacy effectively? | | | |
| 4 | Has the existing birth registration system been implemented effectively? | | | |
| LEGAL FRAMEWORK | | | | |
| This includes the laws, policies and standards governing a DBR system. Without strong, well-enforced data and privacy protection measures, children and caregivers are more vulnerable to privacy violations and unwanted use of their personal data. | | | | |
| 5 | Do laws regulating birth registration meet Plan's standards for protection? | | | Advocate for comprehensive and clear legislation addressing these issues. If greater regulation is not likely – or not likely to be enforced – consider advising against pursuing DBR. |
| 6 | Do national-level data protection laws: A) meet international standards; B) apply to all organisations and agencies that would receive or transmit DBR data; and C) include meaningful penalties for violations? | | | |
| 7 | Are relevant laws and regulations effectively enforced? | | | |

| | RISK ASSESSMENT QUESTIONS | YES/NO/ UNCLEAR | DETAIL | MITIGATIONS TO CONSIDER IF 'NO' OR 'UNSURE' |
|---|---|---|---|---|
| | STAKEHOLDERS | | | |
| | **Implementing partners** | | | |
| | Implementing partners are the government agencies, private companies, non-governmental organisations, and other bodies that play some role within a DBR implementation. These roles could include direct registration, data management, or system administration. These partners must have the technical knowledge and expertise, organisational capacity, and incentives to implement DBR safely. | | | |
| 8 | Do potential implementing partners have a clear mission and high ethical and data protection standards? | | | Avoid working with partners who are not aligned on mission and do not express willingness to uphold key standards. Make these elements clear in partner agreements. |
| 9 | Have all partners demonstrated they can manage data and programme staff well? | | | Provide capacity-building and accountability measures, e.g., training and third party support. If a key partner has limited management capability, develop a strong mitigation plan before pursuing DBR. |
| 10 | Do implementing staff and other participants have strong disincentives to misuse birth data? | | | Address through accountability measures, data protection mechanisms, and performance incentives. Monitor during implementation. |
| 11 | Do influential individuals within implementing partners support child-centred DBR goals and security measures? | | | Define strategy to mitigate the influence of actors in opposition to implementing partners. Consider concessions or compromises to win buy-in from these actors. |
| 12 | Do implementing partners include experienced legal advisers who can identify child protection risks in the legal framework around DBR? | | | Ensure expert legal advisers are closely engaged throughout system design. |
| 13 | Do potential technology partners have experience in implementing CRVS and/ or ICT4D programming? | | | Such experts can accurately analyse technology-related risks in context. They should advise DBR planning and system design, and monitor implementation quality. Vet these experts for expertise and fit with lead implementing partner. |
| | **Families (parents, caregivers and children)** | | | |
| | Failure to address the needs and constraints of families may lead to their exclusion, or allow their data to be used against their wishes. | | | |
| 14 | Is the population generally aware of the risks of digital information sharing? | | | Consider awareness-raising activities, and ensure that informed consent procedures for families reflect awareness of risks. |
| 15 | Are there positive relations between the social groups of implementers and families? | | | Choose implementers with linguistic or cultural similiarities to families in a given location; include sensitivity training for implementers; conduct trust-building exercises prior to/during implementation. |

| | RISK ASSESSMENT QUESTIONS | YES/NO/ UNCLEAR | DETAIL | MITIGATIONS TO CONSIDER IF 'NO' OR 'UNSURE' |
|---|---|---|---|---|

INFORMATION AND IDENTITY MANAGEMENT

### Information governance

'Information governance' is the system by which an organisation manages information and data, defining the authority and decision-making structures around the optimisation, security, quality, and use of data. Without clear, robust and context-appropriate information governance structures, DBR data may be compromised (exposed, corrupted, misused, stolen, lost, or made unusable).

| | | | | |
|---|---|---|---|---|
| 16 | Are all implementing partners and data recipients familiar with concept of information governance and have they employed it previously? | | | Educate leadership, train staff and/or bring in third-party capacity. If inability/ unwillingness to ensure approrpriate information governance system is severe, consider advising against DBR. |

### Identity management

Identity management involves the ability to verify that individuals using a system are who they claim to be, and managing their access to information and/or services based on their verified identity. Without strong and implementable identity management systems in place, the DBR system will not be able to effectively restrict or track access to the process or birth data.

| | | | | |
|---|---|---|---|---|
| 17 | Does a reliable identity management and verification system(s) currently cover all prospective system users? | | | These elements are necessary for DBR implementation. If weakness of either is severe, advise against DBR until reliable identity verification is possible. |
| 18 | Is there a public key infrastructure (PKI) allowing for reliable electronic identity verification? | | | |

EVALUATION & SUMMARY

### Significant risks

Use this space to record the most significant risks from the questions above (those marked 'no' or 'unclear').

### Existing mitigations

Use this space to record mitigations that are already being implemented to address the significant risks.

### Further mitigations to be taken

Identify which significant risks are not addressed by existing mitigations. Use examples from the 'Mitigations to consider if 'no' or 'unsure'' column above. Record the further mitigations that should be implemented in the future.

# B. During system design

This section covers risk factors related to the design of a DBR system. Use these questions as a guide while designing a system, or to assess a fully designed DBR system. Either way: Be sure to complete Tab A, 'Before engagement', first. Then, for each risk question below, answer yes/no/unclear and add details. Then, summarise the risks, existing mitigations, and planned future mitigations at the bottom.

| | RISK ASSESSMENT QUESTIONS | YES/NO/ UNCLEAR | DETAIL | MITIGATIONS TO CONSIDER IF 'NO' OR 'UNSURE' |
|---|---|---|---|---|
| | STAKEHOLDERS | | | |
| | **Implementing partner capacity** | | | |
| | Implementing partners are the government agencies, private companies, non-governmental organisations, and other bodies that play some role within a DBR implementation. These roles could include direct registration, data management, or system administration. These partners must have the technical knowledge and expertise, organisational capacity, and incentives to implement DBR safely. | | | |
| 1 | Is the DBR system embedded in the civil registry authority or similar national-level agency? | | | Advocate for this inclusion. Centralise the administration of the DBR system to the extent possible. |
| 2 | Does the lead implementing agency have the capacity to manage the system, with only limited reliance on third parties whose participation and access to data may be difficult to control? | | | Advise on/assist in developing capacity-building plan that can make DBR locally implementable over the long term. |
| 3 | Is the DBR system integrated in overall CRVS strengthening? | | | Pursue integration. Include mitigations regarding data-sharing protocols, technology choice, management arrangements, etc. to align DBR with CRVS systems and address disparities. |
| 4 | Is the DBR system included in national ICT strategy or similar initiative? | | | Advocate for such institutional ICT capacity building. Use technology in DBR that government agencies and other data users can currently support. |
| | **Implementing partner agreements** | | | |
| 5 | Do the implementing partners have: A) clear privacy and data protection protocols that match international standards; B) clear roles, responsibilities, and restrictions; and C) coordination and communication protocols that support accountability? | | | Structure partner agreements and workplans to ensure that they clearly define data ownership, cover gaps in the legal framework, and restrict all partners and other data recipients from selling, improperly storing, de-encrypting or otherwise using messages, birth data and metadata collected by the system. Cross-border partnerships should be governed by the jurisdiction with the strongest legal protections. |
| 6 | Are there restrictions on use of DBR system data by non-implementing third parties (e.g., other government agencies or firms that can access data from the system)? | | | Include such third parties in binding agreements regulating data use where possible. Ensure that third parties are legally accountable for adhering to responsible data use standards. |

| | RISK ASSESSMENT QUESTIONS | YES/NO/ UNCLEAR | DETAIL | MITIGATIONS TO CONSIDER IF 'NO' OR 'UNSURE' |
|---|---|---|---|---|
| **Implementing partner staff** | | | | |
| 7 | Do implementing partners' staff and volunteers have the technology skills and necessary knowledge for their roles? | | | Address through resourcing, education, choice of implementer, choice of technology, or other means as appropriate. |
| 8 | Do implementing staff have incentives to execute their roles correctly? | | | Build in incentives through good management practices, such as appropriate compensation, supportive working environments, and job stability. |
| 9 | Are there multiple accountability and quality assurance checks on implementing staff? | | | Ensure that checks cover data collection, transmission, storage and sharing. Tailor checks for registration agents, implementing partner staff, and third-party staff as appropriate. Draw on lead implementing agency and legal means to enforce accountabilty. |
| 10 | Are registration agents required to obtain informed consent from caregivers/parents prior to registration? | | | Create protocols for administering and documenting informed consent, and monitor their implementation. |
| **Family consent and access** | | | | |
| 11 | Is information for consent conveyed to families in understandable and relevant formats/manners? | | | Test and refine consent procedures and materials. |
| 12 | Do families who do not give consent or are not comfortable with DBR have other registration options? | | | Allow families to refrain from providing potentially sensitive data. Include information about how to register complaints or concerns regarding DBR with authorities. |
| 13 | Do families have necessary knowledge and technology to access birth data they are authorised to? | | | Advocate for or implement awareness raising as appropriate. Change or adapt DBR technologies used, if needed, and make non-digital options available where possible. |
| INFORMATION AND IDENTITY MANAGEMENT | | | | |
| **Information governance framework** | | | | |
| 14 | Is there an information governance framework establishing implementing partner authority, DBR decision-making structure, and accountability measures? | | | Support creation of a framework that meets conditions defined in the following questions. Ensure that it applies to all partners. Build lead implementing partner's capacity to administer it. |
| 15 | Are the framework and its technology appropriate for the context? | | | Build capacity among implementing partners to fulfil framework standards. Adapt technologies to suit local needs through custom software design, choice of device, etc. |

'Information governance' is the system by which an organisation manages information and data, defining the authority and decision-making structures around the optimisation, security, quality, and use of data. Without clear, robust and context-appropriate information governance structures, DBR data may be compromised (exposed, corrupted, misused, stolen, lost, or made unusable).

| | RISK ASSESSMENT QUESTIONS | YES/NO/ UNCLEAR | DETAIL | MITIGATIONS TO CONSIDER IF 'NO' OR 'UNSURE' |
|---|---|---|---|---|
| 16 | Are secure data management policies clearly defined in the framework and understood by partners? | | | Translate standards and protocols into organisational policy among all partners; coordinate training and monitoring checks to ensure protocols are understood and practised. |
| 17 | Does the framework establish strong data quality controls (e.g., error detection, access tracking, breach detection)? | | | Ensure the framework articulates minimum controls as defined by a data management expert familiar with the context. |
| 18 | Does the framework minimise data collected/stored/shared? | | | Create standards that minimise data based on sensitivity rather than quantity. Collecting more data than necessary for registration (e.g., statistical data) must be justified by the benefit and implementing partners' ability to secure it. |
| 19 | Is there a plan for monitoring, testing, and revising the framework as needed? | | | Develop a framework monitoring and iteration plan, and assign responsibility for implementing it. |

### Information governance practices

| | | | | |
|---|---|---|---|---|
| 20 | Are there user-specific data access levels to keep data on a strict need-to-know basis? | | | Define these privileges in the information governance framework and ensure execution by implementing partners. |
| 21 | Is statistical data stored separately from birth data where possible, and is birth data subject to higher security protocols? | | | Segment data according to its sensitivity and restrict number of individuals able to access higher-sensitivity data. |
| 22 | Is data anonymised prior to sharing where possible? | | | According to the needs of data recipients, data should be anonymised (aggregated, masked, etc). |
| 23 | Are there cloud-based and local back-up servers? | | | Use both types of back-ups when possible. If feasible, cloud storage should be directly controlled by the lead implementing agency. If not, service-level agreements with the cloud hosting service should clearly specify security standards. |
| 24 | Is there a data recovery plan that will be regularly tested and amended? | | | Create a plan accounting for likely causes of data loss and corruption – e.g., natural disasters, conflict, infrastructure failure. One lead agency staff member should hold responsibility for monitoring, testing and upgrading the plan. |
| 25 | Is DBR data easily integrated with older BR data, decreasing risk of storing it insecurely or corrupting records? | | | Budget for staff time and technology needed to make this integration possible. |
| 26 | Is DBR data in a format compatible with those used by partner agencies? | | | Use standard formats where possible. Harmonising formats can be a part of CRVS/ICT upgrading initiatives. |

| | RISK ASSESSMENT QUESTIONS | YES/NO/ UNCLEAR | DETAIL | MITIGATIONS TO CONSIDER IF 'NO' OR 'UNSURE' |
|---|---|---|---|---|
| **Hardware-based security** | | | | |
| 27 | Are registration agents prohibited from using personal devices for data collection? | | | If agents can use their own devices, record device identifiers (e.g., SIMs) and track to the extent possible. Ensure data collection software is properly installed, password protected, and regularly upgraded. |
| 28 | Will data stored on collection devices be encrypted and wiped regularly? | | | Data management staff should be responsible for verifying that device data has been appropriately deleted. |
| 29 | Are all devices and hardware password/PIN protected? | | | Correct this with password/PIN protocols and technology as advised by technology expert famliar with the context. |
| 30 | Are implementing partner staff restricted from using personal devices and/or email accounts to access and share data? | | | All devices, software and platforms should be enterprise-scale. Prevent implementing staff from using personal technology, with possible exception of registration agents. |
| 31 | Are there appropriate physical security protocols and mechanisms regarding the database? And are they well-known to implementers? | | | Establish security measures, including storage of hardware in access-controlled rooms, rules preventing staff from removing hardware, and device-tracking systems. |
| **Software-based security** | | | | |
| 32 | Does software used by implementers track data transmission when submitting or sharing data? | | | Include this safety feature in all software and ensure that implementers in charge of data management can monitor it. |
| 33 | Are there software-based restrictions on unauthorised data transmissions for sender and receiver? | | | Potential security measures include: requiring digital accounts to receive registration-related communications; allowing staff phones to communicate only with authorised numbers. |
| 34 | Does the database include intrusion prevention and system auditing software, with strong user authentication protocols for access? | | | Include all these security measures in database. If data is maintained in cloud-based storage, agreements with cloud server providers should specify additional security mechanisms. |
| 35 | Are database and data collection software easily customizable and upgradable? | | | Use open source or other customizable software as advised. Build partner capacity to adapt software to local needs. |
| 36 | Is data encrypted during transmission and storage at each stage of DBR? | | | Ensure software encrypts all data, and that encryption used at each stage (and by different partners) meets standards set by expert technology advisers. |

| | RISK ASSESSMENT QUESTIONS | YES/NO/ UNCLEAR | DETAIL | MITIGATIONS TO CONSIDER IF 'NO' OR 'UNSURE' |
|---|---|---|---|---|
| **Identity management** | | | | |
| 37 | Do electronic and manual checks verify identities of all system users throughout DBR process? | | | Use combinations of authentications appropriate to partners' technological capacity. Make implementers accountable for conducting checks. |
| 38 | Are identification requirements for families adapted to their constraints? | | | Allow multiple verification means to get around families' constraints, provided these meet minimum requirements as defined by CRVS and information governance experts. |
| 39 | Is a plan for monitoring, testing, and revising identity management and verification practices in place? | | | Develop a plan that can be implemented system-wide. Ideally, improving DBR verification practices should be integrated with countrywide efforts to strengthen identity management. |
| 40 | Is public access to data limited according to data sensitivity? | | | Construct access restrictions according to a system-wide hierarchy of data sensitivity. Establish multistep processes involving automatic and manual identity verification for those who wish to access identifying or other very sensitive data. |

EVALUATION & SUMMARY

### Significant risks

Use this space to record the most significant risks from the questions above (those marked 'no' or 'unclear').

### Existing mitigations

Use this space to record mitigations that are already being implemented to address the significant risks.

### Further mitigations to be taken

Identify which significant risks are not addressed by existing mitigations. Use examples from the 'Mitigations to consider if 'no' or 'unsure'' column above. Record the further mitigations that should be implemented in the future.

# C. After implementation

This section monitors risks that may have developed since the launch of a DBR system. It builds on the previous two sections, and can be completed once adequate data on DBR system implementation has been collected. Revisit these factors throughout the life of a DBR system to monitor risks. For each risk question below, answer yes/no/unclear and add details. Then, summarise the risks, existing mitigations, and planned future mitigations at the bottom.

| | RISK ASSESSMENT QUESTIONS | YES/NO/ UNCLEAR | DETAIL | MITIGATIONS TO CONSIDER IF 'NO' OR 'UNSURE' |
|---|---|---|---|---|
| | OPERATING ENVIRONMENT | | | |
| | **Political, governance and legal context** | | | |
| | This includes the governance, social, economic, and technological context surrounding a DBR system. These contextual factors can contribute to exclusion of or harm to some familiies through DBR implementation. | | | |
| 1 | Have previously identified contextual risk factors intensified or changed? | | | Consider how adjustments to system design could address these risks. |
| 2 | Has the legal framework changed in a way that impacts child, data, or privacy protection? | | | Advocate for regulatory reform to address new risks. Make adjustments to system design as appropriate. |
| 3 | Has integration with CRVS systems/e-governance initiatives proceeded according to design? | | | Look for opportunities to improve CRVS/e-governance through DBR system implementation or other channels. |
| | STAKEHOLDERS | | | |
| | **Implementing partner capacity** | | | |
| | Implementing partners are the government agencies, private companies, non-governmental organisations, and other bodies that play some role within a DBR implementation. These roles could include direct registration, data management, or system administration. These partners must have the technical knowledge and expertise, organisational capacity, and incentives to implement DBR safely. | | | |
| 4 | Have implementing partners demonstrated that they have the human, financial and technical capacity to effectively implement the system? | | | Address by amending partner agreements, enforcing existing accountability mechanisms or creating new ones, executing partner capacity-building measures, or other mitigations as appropriate. Refer to mitigations addressing implementing partner capacity in Tab B, 'During system design', for more. |
| 5 | Are implementing partners and third parties performing their roles responsibly, abiding by relevant legislation and the terms of their agreements? | | | |
| 6 | Are implementing partners communicating and coordinating roles effectively? | | | |
| | **Family consent and access** | | | |
| 7 | Have families indicated that they are comfortable with the DBR process and security risks involved? | | | Refer to mitigations addressing family consent and access in Tab B, 'During system design', for more. |
| 8 | Have all eligible families been able to participate fully in DBR? | | | |
| 9 | Does feedback or other data indicate that families are successfully able to look up/change data after registration? | | | |
| 10 | Are families representing different social grouping and geographic locations equally able to access birth data once it is availalble for look-up? | | | |

| | RISK ASSESSMENT QUESTIONS | YES/NO/ UNCLEAR | DETAIL | MITIGATIONS TO CONSIDER IF 'NO' OR 'UNSURE' |
|---|---|---|---|---|

INFORMATION AND IDENTITY MANAGEMENT

### Information governance framework

'Information governance' is the system by which an organisation manages information and data, defining the authority and decision-making structures around the optimisation, security, quality, and use of data. Without clear, robust and context-appropriate information governance structures, DBR data may be compromised (exposed, corrupted, mis-used, stolen, lost, or made unusable).

| | | | | |
|---|---|---|---|---|
| 11 | Are framework directives regarding decision-making authority, roles and accountability verifiably being followed? | | | Address with relevant changes to the information governance framework, policies, and practices, plus other context-appropriate mitigations in system design. Refer to mitigations addressing the information governance framework in Tab B, 'During system design', for more. |
| 12 | Are data management and quality control being executed according to the information governance framework? | | | |
| 13 | Are agreements and protocols regarding data usage and sharing being enforced? | | | |

### Information governance practices

| | | | | |
|---|---|---|---|---|
| 14 | Are information management plans being executed successfully, with no evidence that data has been misused, accessed by unauthorised parties, or otherwise compromised? | | | Refer to mitigations addressing information government issues in Tab B, 'During system design', for more. |
| 15 | Are staff data access privileges being followed, monitored, and amended as needed? | | | |
| 16 | Is data anonymised prior to sharing where possible? | | | |
| 17 | Are data backup and recovery plans being monitored and updated as expected? | | | |
| 18 | Has the implementing agency been able to integrate DBR data with existing birth data? | | | |
| 19 | Have partner agencies been able to integrate DBR data with their own systems and formats? | | | |

### Hardware- and software-based security

| | | | | |
|---|---|---|---|---|
| 20 | Have data collection and storage hardware been consistently controlled and kept secure? | | | Refer to mitigations addressing hardware- and software-based security issues in Tab B, 'During system design', for more. |
| 21 | Are software-based security mechanisms being successfully implemented and monitored? | | | |

| | RISK ASSESSMENT QUESTIONS | YES/NO/ UNCLEAR | DETAIL | MITIGATIONS TO CONSIDER IF 'NO' OR 'UNSURE' |
|---|---|---|---|---|
| **Identity management** | | | | |
| | Have identification verification protocols been implemented as designed? | | | Refer to mitigations addressing identity management risks in Tab B, 'During system design', for more. |
| | Have these protocols been tested and refined accordingly? | | | |
| | Have families been able to provide the required means of identity verification? | | | |
| | Have systems to securely provide the public access to select data been implemented effectively? | | | |

EVALUATION & SUMMARY

### Significant risks

Use this space to record the most significant risks from the questions above (those marked 'no' or 'unclear').

### Existing mitigations

Use this space to record mitigations that are already being implemented to address the significant risks.

### Further mitigations to be taken

Identify which significant risks are not addressed by existing mitigations. Use examples from the 'Mitigations to consider if 'no' or 'unsure'' column above. Record the further mitigations that should be implemented in the future.

## 7.2 List of risks and mitigations for each step in the DBR process

| Step | Risks | Mitigations |
|---|---|---|
| 1. Notification and birth data collection | • Unauthorised access to registration system via data collection device.<br>• Data is recorded incorrectly, creating an erroneous record.<br>• Caregivers provide personal data without understanding its uses.<br>• Inflexible systems or other failures may exclude children from registration.<br>• Families are subjected to exploitation or other harm by registration agents. | • Secure devices with strong technology and management protocols.<br>• Ensure registration agents have necessary capacity and are accountable.<br>• Prevent potential abuses in later stages by limiting data collected.<br>• Institute context-appropriate informed consent practices.<br>• Include alternatives for those who are excluded by the digital process. |
| 2. Birth data submission to registry database | • Birth data sent or preliminary confirmation received is exposed to unauthorised parties.<br>• Metadata collected during notification is made available to third parties or other unauthorised users.<br>• Fraudulent data is submitted. | • Include security measures in preliminary registration confirmations.<br>• Encrypt data at all possible points.<br>• Implement strict transmission permissions.<br>• Conclude strong agreements with network operators. |

| Step | Risks | Mitigations |
|---|---|---|
| 3. Data validation and record storage | • Records are intentionally compromised.<br>• Records are lost or compromised due to mismanagement.<br>• New data is incompatible or not integrated with existing data. | • Choose data storage systems with security concerns and institutional context in mind.<br>• Tightly control access and monitor activity.<br>• Include quality assurance mechanisms with a manual or human component.<br>• Promote human capacity to pre-empt violations.<br>• Build necessary capacity for technical upgrades into the system design and budget.<br>• Enable effective data recovery through planning and appropriate technology. |
| 4. Birth record data is shared and distributed | • Data and databases are compromised during sharing.<br>• Shared data is commercialised or used irresponsibly by receiving parties.<br>• Children and caregivers have no agency over how their data is used. | • Codify and enforce strong privacy regulations.<br>• Process data before sharing to minimise exposure.<br>• Strong agreements with shared agencies and partners over ownership, licensing and sharing permissions.<br>• Share via enterprise-scale platforms, software, and devices. |
| 5. Data is queried, checked, and corrected | • Caregivers are unable to access and correct records, excluding children from benefits.<br>• Unauthorised users access and/or alter birth data. | • Make analogue processes available alongside digital ones.<br>• Create strong authentication processes for users accessing data.<br>• Match data display and delivery details to risk potential. |

## 8.1 Suggested resources

### Digitising birth registration and civil registration and vital statistics

**African Programme on Accelerated Improvement of Civil Registration and Vital Statistics:** "Draft: Second Conference of African Ministers Responsible for Civil Registration." 2012.

**Document Security Alliance:** "Call to Action: Birth Certificate Security." 2010.

**HMN:** "The Case for Investment in Civil Registry and Vital Statistics Systems." 2012.

**NAPHIS:** "More, Better, Faster: Strategies for Improving the Timeliness of Vital Statistics." 2013.

**UNICEF:** "Civil Registration Study Tour in Uganda." 2013.

**UNICEF:** "Good Practices in Integrating Birth Registration into Health Systems (2000-2009)." 2010.

**UNICEF:** A Passport to Protection: A Guide to Birth Registration Programming. 2013.

**United Nations Statistics Division:** Civil Registration and Vital Registration Knowledge Base.

**United Nations Statistics Division:** "Principles and Guidelines for Managing Statistical Confidentiality and Microdata Access." 2007.

**US Center for Disease Control:** "Global Program for Civil Registration and Vital Statistics Improvement."

**World Bank:** "An Assessment of LAC's Vital Statistics System: The Foundation of Maternal and Infant Mortality Monitoring." 2008.

**World Health Organisation:** "Strengthening civil registration and vital statistics for births, deaths and causes of death: a resource kit." 2013.

### Technology and protection

**Cash Learning Partnership:** "Protecting Beneficiary Privacy: Principles and operational standards for the secure use of personal data in cash and e-transfer programs." 2013.

**Cloud Standards Customer Council:** "Security for Cloud Computing: 10 Steps to Ensure Success." 2012.

**Dunstan Allison Hope:** "Protecting Human Rights in the Digital Age: Understanding Evolving Freedom of Expression and Privacy Risks in the Information and Communications Technology Industry." 2011.

**Freedom House:** "Safety on the Line: Exposing the myth of mobile communications security." 2012.

**International Association of Privacy Professionals:** Privacy Perspectives Blog.

**International Committee of the Red Cross:** "Professional Standards for Protection Work." 2013.

**ISO/IEC:** "ISO/IEC 27001 - Information technology – Security techniques – Information security management systems – Requirements". 2013.

**ITU:** "Trends in Telecommunication Reform 2013: Transnational Aspects of Regulation in a Networked Society." 2013.

**New America Foundation:** "Dialing Down Risks: Mobile Privacy and Information Security in Global Development Projects." 2013.

**Richard Power:** "Child Identity Theft: New evidence indicates identity thieves are targeting children for unused social security numbers." Carnegie Mellon CyLab. 2011.

**Trustlaw Connect:** "Patient Privacy in a Mobile World: A Framework to Address Privacy Law Issues in Mobile Health." 2013.

**UNICEF:** "Integrated Social Protection Systems: Enhancing Equity for Children."

## 8.2 Endnotes


### Information and identity management

**Data Governance Institute:** "DGI Data Governance Framework."

**HM Government:** "Information Governance Toolkit."

**HM Government:** "Government Cloud Strategy." 2011.

**Inter-American Development Bank:** "Resources on Identity Management."

**Kristina Pitula, Daniel Sinnig, and Radhakrishnan:** "Making Technology Fit: Designing an Information Management System for Social Protection Programmes in St. Kitt." University of the West Indies. 2010.

**Marit Hansen, Ari Schwartz and Alissa Cooper:** "Privacy and Identity Management." Center for Democracy and Technology. 2008.

**Mia Harbitz and Ivan Arcos Axt:** "Identification and Governance Policies: The Legal, Technical and Institutional Foundations that Influence the Relations and Interactions of the Citizen with the Government and Society." Inter-American Development Bank. 2011.

**Pension Watch, HelpAge International:** "Good Practice in the Development of Management Information Systems for Social Protection." 2011.

**Privacy Rights Clearinghouse:** "Database of data breaches."

1. **Sharad Sapra:** "Uganda making progress on birth register." AllAfrica.com, 19 December 2013.
2. **Inter-American Development Bank:** "Newborn Citizens." Accessed 11 January 2014.
3. **UNICEF: "**A Passport to Protection: A Guide to Birth Registration Programming." 2013. Page 11.
4. **Mia Harbitz and Ivan Arcos Axt:** "Identification and Governance Policies: The Legal, Technical and Institutional Foundations that Influence the Relations and Interactions of the Citizen with the Government and Society." Inter-American Development Bank. 2011. Page 27.
5. **Sunil Soares:** "The IBM Data Governance Unified Process: Driving Business Value with IBM Software and Best Practices." 2010. See also: United Kingdom Department of Health: "Information: To Share or Not to Share? The Information Governance Review." 2013.
6. **United Nations General Assembly:** "The Right to Privacy in the Digital Age: Revised Draft Resolution." 2013.
7. **EUR-LEX:** "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data." 1995.
8. **TechTerms.com:** "API."
9. **TechTerms.com:** "Cloud."
10. **TechTerms.com:** "Digital Signature."
11. **TechTerms.com:** "Public Key Infrastructure."
12. **UNICEF: "**A Passport to Protection: A Guide to Birth Registration Programming." 2013. Page 11.
13. **Sharad Sapra:** "Uganda making progress on birth register." AllAfrica.com, 19 December 2013.
14. **Richard Power:** "Child Identity Theft: New evidence indicates identity thieves are targeting children for unused social security numbers." Carnegie Mellon CyLab. 2011; Paul Tentena: "Cyber crime on the increase in Africa." East African Business Week, 31 March 2014.
15. **Edward Moyer:** "Hackers crack major data firms, sell info to ID thieves, says report." CNet, 25 September 2013.
16. **Mwaura Kimani:** "Gone in 12 months; how fraudsters stole $17m from Kenya's banks." The East African, 18 May 2013
17. **Hayley Tsukuyama:** "Target Says 40 Million credit, debit, cards may have been compromised in breach." Washington Post, 19 December 2013. See also: **Alexandrine Pirlot:** "Ignoring repeated warnings, Argentina biometrics database leaks personal data." Privacy International, 10 December 2013.
18. **Carly Nyst:** "The road to surveillance is paved with good intentions – and warning signs." The Guardian, 12 November 2013.
19. **Trustlaw Connect:** "Patient Privacy in a Mobile World: A Framework to Address Privacy Law Issues in Mobile Health." 2013. Page 36.
20. Mia Harbitz and Ivan Arcos Axt. Page 14.
21. **UNICEF:** A Passport to Protection.

22. InfoDev: "e-Government Primer." 2009.
23. United Nations Economic Commission for Africa; African Union Commission; African Development Bank: "Africa Programme on Accelerated Improvement of Civil Registration and Vital Statistics Strengthening." 2012. Page 3.
24. Practitioner interview.
25. Note that this is not always the case, and that technology providers have taken important steps to advance privacy standards.
26. International Committee of the Red Cross: "Professional Standards for Protection Work." 2013. Page 89.
27. UNICEF: "Good Practices in Integrating Birth Registration into Health Systems (2000-2009)." 2010. Page 41.
28. Practitioner interview.
29. Ibid., Page 23.
30. Ibid., Page 16.
31. Practitioner interview.
32. News24: "Bluetooth Devices Easily Hacked." 23 October 2007.
33. UNICEF: "Good Practice," Page 14.
34. UNICEF: "Birth Registration in Ghana – a bottleneck analysis that leaves no child out." 2013. Page 35.ICRC: "Professional Standards for Protection Work." Page 89.
35. ICRC: "Professional Standards for Protection Work." Page 89.
36. UNICEF: "Passport to Protection." Page 28.
37. Marit Hansen, Ari Schwartz and Alissa Cooper: "Privacy and Identity Management." Center for Democracy and Technology. 2008. Page 2.
38. Access: "Access position on the European Commission proposal for a General Data Protection Regulation." 2012.
39. Cash Learning Partnership: "Protecting Beneficiary Privacy: Principles and operational standards for the secure use of personal data in cash and e-transfer programs." 2013. Page 8.
40. Marit Hansen, Ari Schwartz and Alissa Cooper, 2008. Page 43.
41. Trustlaw Connect, Page 37.
42. New America Foundation: "Dialing Down Risks: Mobile Privacy and Information Security in Global Development Projects." 2013. Page 2.
43. Ibid.
44. Center for Health Market Innovations: "RapidSMS Nigeria."
45. GSMA: "The Mandatory Registration of Prepaid SIM Card Users." 2013. Page 7.
46. See, for example: Resistencia Honduras: "Election database shielded after cyber attack in Honduras." 21 December 2013. See also: Privacy Rights Clearinghouse: "Chronology of Data Breaches."
47. Cloud Standards Customer Council: "Security for Cloud Computing: 10 Steps to Ensure Success." 2012.
48. UNICEF: Good Practices, Page 23. Plan International: "Count Every Child: the Right to Birth Registration." 2009. Page 68.
49. UNICEF: "Birth Registration in Ghana." Page 31.
50. UNICEF: "Birth Registration in Ghana." Page 43. Plan International: "Count Every Child." Page 57.
51. Gus Hosein and Carly Nyst: "Aiding Surveillance." Page 25.
52. Mia Harbitz and Ivan Arcos Axt. Page 21.
53. ITU: "Trends in Telecommunication Reform 2013: Transnational Aspects of Regulation in a Networked Society." 2013.
54. NAPHIS: "More, Better, Faster: Strategies for Improving the Timeliness of Vital Statistics." 2013. Page 23.
55. Document Security Alliance: "Call to Action: Birth Certificate Security." 2010. Page 3.
56. Quest Technology Management: "Backing up and Recovering your Business Data: 10 Best Practices." 2011.
57. Gus Hosein and Carly Nyst: "Aiding Surveillance." Page 25.
58. Mark Sullivan: "Data Snatchers! The booming market for your online identity." PC World. 26 June 2012.
59. Expert interview.
60. Civil Service World: "Vital Statistics." 29 October 2013.
61. Cash Learning Partnership, 2013. Page 9-10.
62. Ibid.
63. HM Government: "Government Cloud Strategy." 2011. Page 5.
64. Seven Days: "Born in Vermont? Identity Thieves Want Your Birth Certificate." 29 June 2011.
65. Practitioner interview.
66. ICRC: "Professional Standards for Protection Work." Page 89.

COVER PHOTO: ASAD RASSEL/PLAN INTERNATIONAL

## About Plan International

Plan has been working for and with children for more than 75 years. We currently work in 50 low and middle income countries across Africa, Asia and the Americas to promote child rights and lift millions of children out of poverty.

We focus on the inclusion, education and protection of the most marginalised children in partnership with communities, local and national government and civil society.

Plan works with more than 90,000 communities each year, covering a population of 78 million children.

Plan is independent, with no religious, political or governmental affiliations.

**Plan**

International Headquarters
Dukes Court
Duke Street
Woking
Surrey GU21 5BH
United Kingdom

t +44 (0) 1483 755155

f +44 (0) 1483 756505

**plan-international.org/birthregistration**

Plan