eRegistries Initiative

eRegistries

governance guidance toolkit

June 9 2016

preface

The eRegistries for maternal and child health is a global initiative to improve data quality and data collection techniques for maternal and child health. The eRegistries Initiative is a comprehensive health surveillance package designed to document, manage, and communicate reproductive health information to a broad range of stakeholders.

Within this general report, we make suggestions that could be useful to public health officials and/or authorities based on the Situation Analysis Tool they have completed regarding legislation and governance. This will help to start the planning to develop the infrastructure that is needed for an eRegistry for maternal and child health. This draft of the document may be modified so we would be pleased if this material is seen not the final version.

We welcome any comments or suggestions on how to improve it.

Jane Kaye, LLB, DPhil
Jessica Bell
Colin Mitchell
Andelka Phillips
University of Oxford

Sonja Myhre, MsPH, PhD
Norwegian Institute of Public Health

12th March 2015

acknowledgements

We would like to thank the following individuals for their careful reading and thoughtful comments and suggestions on earlier drafts of this document. We are grateful to: Margunn Aanestad at the University of Oslo's Department of Informatics, Herbjørn Andresen at the College of Applied Sciences on the Faculty of Social Sciences, Isabelle Budin Ljøsne at the University of Oslo's Centre for Medical Ethics, and Heidi Beate Bentzen at University of Oslo's School of Law.

contents

abreviations

CoIA	United Nations Commission on Information and Accountability for Women's and Children's Health
DHIS	District Health Information System
DPA	Data Protection Agency or Authority
EHR	Electronic health record
EMR	Electronic medical record
FP	Family planning
HeLEX	Health, Law, & Emerging Technologies Center
HISP	Health Information System Program
ICT	Information communication and technology
IMR	Infant mortality rate
IT	Information technology
PHI	Personal health information
MCH	Maternal and child health
MMR	Maternal mortality rate
NIPH	Norwegian Institute of Public Health
OECD	Organization for Economic Cooperation & Development
RMNCH	Reproductive, maternal, newborn & child health
SIM	Subscriber identity module
UiO	University of Oslo
UN	United Nations
UNFPA	United Nations Population Fund
UNICEF	United Nations Children's Fund
VPN	Virtual Private Network
WHO	World Health Organization

definitions

The definitions provided below are explicitly for the purposes of this document only and do not aim to fully encompass all attributes of these complex terms.

confidentiality The understanding between a health care professional or provider and a patient or authorized representative that all personal information communicated during health care is deemed private and only disclosed if permitted by the patient.

data security The systematic protection of data from unauthorized access, use, disclosure, modification, recording or destruction by means of administrative, organizational, technical, and physical security safeguards to ensure the confidentiality, integrity and availability of personal data.

eHealth The transfer of health resources and health care by electronic means (i.e., the Internet, telecommunications) and/or the use of e-commerce and e-business practices in health systems management (as defined by WHO).

eRegistry for MCH An electronic, organized system for the collection, storage, retrieval, analysis, and dissemination of information on health determinants and outcomes for individual persons, focusing on maternal and child health, with the purpose of supporting health care provision, public health surveillance, and research.

eRegistries framework The eRegistries framework encompasses the establishment, implementation, and management of electronic registries for reproductive, maternal and child health, including ethical and legal guidance; evidence-based indicators; implementation tools; customizable software; and analysis and dissemination tools.

eRegistries Initiative Located at the Norwegian Institute of Public Health, the eRegistries Initiative provides technical assistance for, and research concerning the implementation of the eRegistries framework.

mHealth The use of wireless or mobile phones and other devices to facilitate health and/or medical care and public health practices.

privacy Seclusion, freedom from disturbance or interference.

patient registry An organized system for the collection, storage, retrieval, analysis, and dissemination of information on health determinants and outcomes for individual persons for a specific public health purpose to support health care provision, public health surveillance, and research.

01 – introduction

Globally, lack of available and quality maternal health data has hampered progress, understanding, and efforts to reduce maternal mortality and morbidity, particularly in low-income settings where the need is greatest.[1-5]

Recognizing this gap, the Commission on Information and Accountability for Women's and Children's Health (CoIA) developed recommendations to strengthen data information systems related to vital events and health indicators.[6]

The urgent call for more and better maternal health data has also emanated from the top leadership of numerous global health agencies including the WHO, the UN, the World Bank, UNICEF, and UNFPA, to name a few.[7-10] Highlighting the value of maternal data to address mortality, Melinda Gates has also echoed this sentiment in recent high profile editorials.[11,12]

Historically, population-based, health surveillance data has assumed an integral role in the field of public health.[13-15] Similarly, patient medical registries have established a centuries' old precedent of collecting individual health data with the intent to serve the greater common good.[16-18] Underscoring this concept, Gissler aptly noted, "the cornerstone of the national health information systems is register information"(pg. 171),[19] - a primary premise underlying the longstanding Nordic tradition of collecting registry data.[19-23]

Field studies and research applying the registry concept to maternal health has demonstrated unique potential.[24,25] According to a 2015 report by Harvard's Maternal Health Task Force, the most frequently mentioned emerging opportunity for post-2015 maternal health in low income countries was the potential of information and communication technologies applied to maternal health challenges.[26]

The eRegistries Initiative, based at the Norwegian Institute of Public Health, is dedicated to improving health data with the aim of improving quality of care and health outcomes. The eRegistries Initiative provides technical assistance and research on the implementation of the eRegistries framework which encompasses the establishment, implementation, and management of electronic registries for reproductive, maternal and child health.

5 core components:

1. ethical and legal guidance
2. evidence based RMNCH indicators
3. implementation tools
4. customizable software
5. analysis and dissemination strategies

CORE COMPONENTS

The eRegistries framework is comprised of **five core components**, namely: ethical and legal guidance, evidence-based RMNCH indicators, implementation tools, customizable software, and analysis and dissemination strategies. To address the first core component on ethical and legal guidance, the eRegistries framework developed the eRegistries Governance Guidance Toolkit which outlines what is needed in terms of a governance and regulatory structure to establish, operate, and maintain a registry dedicated to reproductive, maternal, newborn, and child health (RMNCH). Although the intrinsic value of health registry data has been widely recognized[27,28], few all-purpose, general guidelines or common principles for governing registries are available or have been published to date.[29] Thus, this Toolkit addresses contemporary registry issues that have not been formally articulated in a cohesive manner.

The eRegistry for maternal and child health is built on the District Health Information System (DHIS2) platform - an open source software designed for the collection, validation, analysis, and presentation of aggregate and transactional data using mobile phone, internet and cloud services. Utilizing this technology, the eRegistries Initiative leverages the features of this architecturally secure platform which has been proven in many different contexts. As of 2015, DHIS2 is operational in more than 40 developing countries throughout Africa, Asia and Latin America making it one of the largest and most successful global health information platforms.

The eRegistry for maternal and child health is designed to collect health information during the antenatal phase and follow women through the intrapartum and postpartum period thus documenting the full spectrum of maternal and child health care as designated by the World Health Organization's Essential Interventions for RMNCH.[30] This comprehensive, panoramic perspective (as compared to singular 'snapshot' views) is vital to understanding when and where women and children experience health problems.[3]

A unique feature of the eRegistry approach is that it captures health data at the primary care level and facilitates feedback to public health officials, health care providers, and women and their families. By merging traditional health registry surveillance practices with information technology strategies, the eRegistry has the ability to disseminate information to a wide range of stakeholders that can drive better health decisions, behaviors, and ultimately, policies.

The rapid growth and proliferation of health information technology, however, has dramatically increased the potential for unintended consequences, particularly concerning data privacy and security. Although the tension between public health registry data and individual privacy interests has been debated extensively[31-37], these issues are particularly compelling in countries with limited public discourse or regulatory infrastructure.[38]

> ***There may be no greater threat to the operation of a [registry] than an actual or perceived breach of confidentiality. In fact, an actual or perceived breach of confidentiality in one registry may threaten all registries.***
>
> ***(pg. 125).***[43]

Technological advances have far outpaced progress in data protection legislation and governance, particularly in low income and resource-constrained settings.[39] A study conducted by the WHO Global Observatory for eHealth, for example, found that many developing countries are not well-equipped to handle ethical and legal challenges that often accompany technological advances of accumulating and managing digitized data.[40] Likewise, a systematic review of health informatics in developing countries noted the formidable challenges experienced by many countries.[41]

Finally, lack of attention to legal and ethical issues in the mobile health (mHealth) field in developing countries resulted in a commissioned report assessing the array of data privacy and security issues that concern personal health data collected via mhealth applications.[42]

The alarming trend of medical identity theft offers another compelling reason for securing a robust regulatory framework.[44] According to the Identity Theft Resource Center, the highest number of breaches occurred in the medical/health care industry (42.5%) in 2014 followed by the business sector (33%), government and military (11.7%), education (7.3%), and lastly, banking, credit or financial institutions (5.5%).[45]

Although the common perception of identity theft typically involves using a person's identity to acquire financial or material resources, obtaining medical care under the guise of someone else's identity is on the rise with substantial negative repercussions for victims. In

terms of total cost, average length of misuse, and average time of detection, medical identity theft incurs the most across all categories.[44]

Given the importance of ensuring that an eRegistry is conducted in a lawful and ethical manner, this toolkit provides an overview of ethical and legal issues that must be considered as well as governance strategies that will protect women and children's health information. Reproductive health data, by its nature, is highly sensitive given that it may concern HIV status, pregnancy terminations, or other potentially stigmatizing or incriminating personal information.

Careful planning and caution, therefore, is essential. Moreover, women and children in low income settings represent particularly vulnerable populations that demand the utmost care and consideration with respect to their privacy and confidentiality.

The purpose of this governance toolkit is to identify best practices and discuss potential benefits of regulations, guidelines, and legislation. While there is an international precedent of collecting health data for public health surveillance purposes, the current challenge is to achieve an appropriate balance between public health and data protection.[32] Legislation and regulations may assume a significant role in this process. A registry's statement of purpose, for example, can explicitly limit a registry's scope to serving a public health purpose thereby excluding any possibility of using registry data in criminal or legal cases. By setting such parameters, women and children's data is safe from incrimination.

Although there is a vast body of literature on specific patient, product, and disease specific registry protocols[46-54], the few publications to explicate on general registry issues are limited due to their distinct U.S-based vantage point.[17,55] Due to the dearth of universal guidelines on regulatory mechanisms for health registries, the development of this toolkit has relied on an extensive review of standards, methods, and procedures established by a broad range of registry systems including vital statistics[19,56-59] (i.e., birth), cancer[43,50,60-64], clinical quality registries[46], chronic disease[54], and diabetes.[52,65]

Each of these unique registry traditions provides a unique and valuable perspective that has been woven together to form a basic RMNCH registry governance framework. In sum, the aim of creating effective policies, procedures, and protocols for governance and security is vital to the transparency, management, and success of an eRegistry for maternal and child health.

FIGURE I: KEY REGISTRY ACTIVITIES

Figure I provides an overview of the different stages that are covered in this guide. Legal and Ethical considerations are considered in relation to the establishment, operation, use and maintenance of a regisry.

COUNTRY ADAPTATION

A substantial challenge of developing governance guidance in a global context is the inherent diversity in how different countries approach law, ethics, and health. Cultural differences in how issues of confidentiality, privacy, and security are managed will influence laws, policies, and protocols. A country's legal, ethical and cultural parameters will significantly affect the process, priorities, and policies that are developed. Thus, it is essential to carefully evaluate and assess the legal, regulatory, ethical, social and cultural environment and adapt this guidance accordingly.

Transplanting legal language and/or documents from one country to another is not advisable. Country level policies should be rooted in the institutional fabric. Translated adaptations from the outside are not able to embrace subtle social or cultural mores that can impact both acceptance and compliance. Thus, the intent of this toolkit is not to suggest a single, one-size-fits-all approach, but rather to advocate best practices and identify a foundation of relevant international instruments that can help inform this process.

FIRST STEPS

A recommended first step is to complete the eRegistry's Situation Analysis Tool in order to assess the existing structures and factors that concerwwn an eRegistry for maternal and child health. For more information, see: **http://www.fhi.no/hRHR/NeedsAssessmentTool.pdf**.

This guide provides a series of steps and information that aims to provide a basis for establishing an eregistry for maternal and child health. Each country will have to conduct their own evaluation before setting up an eregistry due to the complexity of the legal requirements in their own jurisdiction. This is a guide only and should not be considered as legal advice. Each country or setting will need to carefully consider specific legal requirements such as constitutional codes and comply with local and regional regulations.

02 – how to use this guide

format

The document is designed to provide practical guidance in developing essential eRegistry policies, procedures, and protocols. This toolkit is divided into sections that address important legal and ethical topics that must be considered in establishing an eRegistry. A brief synopsis of each topic explains the relevance and rationale and is followed by examples of statements that may facilitate registry documentation.

examples of statements

Suggested text is provided in bold font in text boxes. Exact wording should be tailored and customized to accommodate each country's legal, cultural and social contexts as it pertains to reproductive, maternal and child health. A summary of eRegistry documentation is noted in Appendix I.

resources

Where appropriate, supplementary resources, references, and and/or hyperlinks are noted at the end of each section.

inclusion/ exclusion

Not all topics are required or necessary in every setting but, rather, will depend on the individual circumstances of each country. Careful consideration of the relevance of each topic should be evaluated for inclusion.

revision management

Establishing an eRegistry document containing policies and procedures is an evolving process that should involve revisions, updates, and periodic review in response to fluctuations in the legal, political and/or social environment. To document changes and revisions, the first page of this toolkit provides a record that can be completed and signed by authors and reviewers in order to track changes and amendments over time (See page ii).

03 – regulatory environment

Law is varied and consists of different legal 'instruments' that have varying levels of application and impact on an international, national, or regional level.

At a domestic level, countries will establish laws that have full legal force that means they are directly applicable (i.e., binding) to that particular activity within that particular country. These are called 'national legislation' and are created by the State.

Every country will have national legislation that is legally binding, as well as other guidelines, codes of practice, and policy documents that steer and guide activities. The latter do not usually have 'legal' impact. In other words, they are not legally binding. They are, therefore, often referred to as 'soft' law and come from a range of actors including government, funders, or professional authorities.

At the European level, legal documents are either 'directives' or 'regulations'. Regulations are directly applicable to the member states that are part of the European Union and have immediate force. Countries that are members of the EU, therefore, do not have to do anything further. Directives, on the other hand, have to be implemented into national (i.e., domestic) legislation that means each country has to amend or create law in their own country in order to comply with the requirements of that particular directive.

At an international level, there are many documents that have been developed to harmonize and guide all countries on a particular activity. These international legal documents are not necessarily legally binding but it is strongly recommended that countries abide by them in order to promote best practice across the world. If countries agree to abide by these international laws, the law becomes legally binding and the country can be held to the standards contained in the piece of legislation. Alternatively, they can be used as a guide.

Together, these varied instruments make up the 'regulatory environment'. Before initiating an eRegistry for maternal and child health, it is important to develop a broad understanding of the nation's current registry environment for opportunities, gaps, risks and barriers. Specifically, the process may involve identifying opportunities for re-using, modifying, or sharing components, pinpointing gaps that need to be addressed, and ascertaining potential risks or barriers in doing so.

3.1 REVIEWING THE REGULATORY ENVIRONMENT

Every country has different laws and regulations that shape how information may be collected, stored and used for certain purposes, as well as many different bodies that make decisions on when and how information can be collected and used. In many countries, this will also be the case at the state or local level. There are also 'softer' (or non-legal) forms of regulation that include policy documents and guidance from a range of actors such as governments, funders, or professional authorities that will also be important in shaping the development of a registry. All of these considerations constitute what can broadly be called the 'regulatory environment.'

As a first step in setting up an eRegistry for maternal and child health, it will be helpful to audit the local, country specific, regulatory environment relevant to starting and running an eRegistry as this will identify areas of regulation and governance that are already covered and will highlight areas that require further consideration.

3.2 MAPPING THE REGULATORY ENVIRONMENT

Because each country is different, there is no pre-determined way to go about mapping the regulatory environment. It is possible, however, to identify some of the major areas of law, regulation and authority control that are likely to be important for registries and can be good starting points. These can be broken down into two main areas; relevant law and regulations and relevant bodies and their guidance.

3.2.1 LAW AND REGULATIONS

PRIVACY

Some countries will have law and legislation on privacy in general (as well as constitutional protection of a right to privacy) that will make it a default position that health information should not be shared without patient consent. In many countries, for example under Australia's Privacy Act, there is a broad exception in the 'public interest.' It is important to understand the scope of this exception in each country to understand if it includes the work of a registry.

DATA PROTECTION

Similar to privacy, there may be general law on data protection that limits the sharing and processing of health data but may allow its use in the public

interest. For example, Ghana has a Data Protection Act (2012) that allows the processing of health data without consent on health grounds. On top of this, data protection laws may set out principles on how data is dealt with fairly and transparently and limited to the purpose for which it was collected (this is the case in the EU and countries with equivalent protection- something the EU law requires before sharing data abroad). To date, more than a hundred data privacy laws that have been enacted throughout the world including many countries in Africa and Asia underscoring the growing global concern and importance.[66,67]

MEDICAL INFORMATION OR HEALTH RECORD

Law on disclosure of health or patient information may supplement or exist in the absence of wider data protection legislation. Nigeria's Medical and Dental Practitioners Act (Cap.M8, Laws of the Federation of Nigeria, 2004), for example, sets out a legal basis for a National Code of Ethics that requires all communication in the course of treatment to remain confidential unless disclosure is compelled by law. These sorts of regulations will shape whether patient consent is needed as well as whether approval is needed from certain authorities before information can be collected or, as in case of Nigeria, whether a legal mandate is required to collect certain types of patient information.

PUBLIC HEALTH OR DISEASE SURVEILLANCE

Laws pertaining to public health, health registries, or disease surveillance (i.e., cancer) or administrative orders issued by statutory agencies (i.e., Ministry of Health or a provincial health authority) may be relevant. (The WHO's International Digest of Health Legislation (IDHL) is one potential resource available here: http://apps.who.int/idhl-rils/frame.cfm?language=english).

SPECIFIC TYPES OF INFORMATION

It is often the case that specific areas of sensitive health information are governed by their own rules. The law governing testing for and collection of data on HIV and AIDS is an example. Tanzania's HIV and AIDS (Prevention and Control) Act of 2008 protects the results of HIV testing as confidential. Similar rules may apply to other sensitive issues, i.e., abortion records. In these cases, it may be that there will be a public interest exception to confidentiality or it might mean that legislation is required to legitimize collection of this data in a registry.

3.2.2 RELEVANT AUTHORITIES AND GUIDANCE

RESEARCH APPROVAL

Legislation may be in place to regulate health research and this will often require an approval or license from a specific body in order to collect and process patient information. This is commonly a requirement to seek ethical approval from an ethics authority. Even if patient consent is not required, the ethics authority will consider the use of the information and safeguards and governance structures in place to protect it. This is an area where the guidance of national or local ethics authorities will be very important.

DATA AND INFORMATION AUTHORITIES

In many cases where there is a national data protection law, data or information authorities are put in place to govern how data is used. Their guidance is important in interpreting rules and sometimes their approval may be necessary for the use of sensitive data.

OTHER BODIES AND GUIDANCE

There are likely to be a variety of other bodies who in some way govern the collection or use of sensitive health data. These could be very general bodies like the Health Coordinating Council in Ghana, which is responsible for making sure that data flows between healthcare providers and there is a coordinated strategy for health care delivery and monitoring, or much more specific bodies like individual hospital committees with control of patient records.

Human rights commissions who issue guidance on protection of certain rights (e.g., the rights of women, right to health, privacy etc.) may also be important. This is not an exhaustive list of potential parts of the regulatory environment for registries, however, so there are likely a range of other relevant sources and authorities in many countries.

04 - legal framework

"An understanding of the appropriate legislation and ethics with respect to clinical data is a prerequisite for establishing any clinical registry" (pg. I) [68]

"Fundamental to any large clinical registry is its ability to function within the parameters laid out by the legal framework governing it. Failure to understand or comply within this framework can be a terminal event for any registry and could potentially have criminal or political repercussions. Issues that fall under this umbrella include data privacy and protection, ethical use of data and intellectual property right (p. I)." [68]

Due to the variation in legal systems worldwide, each registry must operate according to the law of the country where it is located. An important first step is to identify all relevant legislation and regulations that could apply to the registry in order to appreciate the extent of legal requirements and obligations. Relevant areas of law may include vital statistics, public health, freedom of information, privacy, health information, health administration, and personal health information and data collection.[63]

The reproductive health registry must be able to collect health data on reproductive care lawfully. This can be mandated in one of the following ways:

- **Specific legislation** (or amended legislation) relating to health registries. This could be enacted by a state, provincial/territorial legislature, Congress or Parliament.[43]
- **Regulations or rules** developed by a responsible authority such as the Ministry of Health. The regulations or rules govern the activity and they often come from a power given by law.[43]
- **Guidelines** developed by other bodies in society which healthcare professionals follow (i.e. as part of a professional society).

In a number of countries, there may be legislation that applies, in a general way, to registries of data collection for public health purposes. When there is general legislation, guidelines can be used as a way to describe the specific rules that may apply to registries. An advantage of this approach is that guidelines can be changed easily with new circumstances. The benefit of having legislation or guidelines that apply specifically to registries, is that it is easy for people to find the information that they need to understand how the registry works and what the rules are located.

The experiences of other registries have shown that developing government-issued policies is useful because health care providers and institutions are more likely to take notice of rules that are required by the government rather than requests from the registry itself.

4.1 GOVERNANCE COMPONENTS

Once existing legislation or regulations have been identified, it will be possible to evaluate the content to see whether it can be improved or amended.[69] If it is not possible to do this, these essential governance components could be incorporated into guidelines that are written especially for the registry. Also, key factors to obtain broader support and acceptance include demonstrating governmental support through the presence of such policies or directives and showing the value of the registry data.[69]

4.2 LEGISLATIVE COMPONENTS

Legislation or regulatory instruments concerning health registries address these topics[70]:

I. Purpose of the registry
2. Legal, fiscal and operational responsibility
3. Reporting requirements and enforceability
4. Data quality and standards
5. Data security, confidentiality policies, and public access
6. Public Engagement

The contents of legislation should describe, first and foremost, the purpose and scope of the registry. Secondly, a responsible entity should be identified that will assume legal, fiscal and operational responsibility of the registry. The obligatory nature of reporting by providers and institutions to the registry should be noted with a clearly stated timeframe. Enforcement protocols regarding reporting should describe consequences or penalties for non-compliance. Data privacy protection, storage, and retention of personal health information as well as assurance of confidentiality must ensure the privacy and confidentiality of both individuals and reporting sources is protected.

The conditions regarding the release of registry data (i.e., to who, when, how, and in what format) should be described. These should pay attention to the public availability of aggregate data, and the explicit policy regarding restricted access to confidential data. Data quality and standards should be clearly defined in terms of completeness, timeliness, and quality.[43] Similarly, the terms of patient access to their own personal data and allowances for change or deletion may be mentioned. Lastly, public engagement can be addressed to ensure acceptance, support, and trust from the public.

eRegistries Initiative

THE FOUNDATIONAL INTERNATIONAL LEGAL INSTRUMENTS INCLUDE:

Medical Research

- Declaration of Helsinki (World Medical Association, 1962)
- Operational Guidelines for Ethics Committees that Review Biomedical Research (WHO, 2000)

Right to Family Life and Health

- International Covenant on Economic, Social and Cultural Rights (ICESCR) (United Nations General Assembly, 1966)
- Rights for Women
- Convention on the Elimination of All Forms of Discrimination Against women (CEDAW) (United Nations General Assembly, 1979)

Rights for Children

- Convention on the Rights of the Child (United Nations General Assembly, 1989)
- Right to Privacy
- Universal Declaration of Human Rights (United Nations General Assembly, 1948)

Information Law

- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CoE, 1981)
- Guidelines Governing the Protection of Privacy and Transborder Data Flows of Information (OECD, 1981)
- European Union Data Protection Directive 98/46/EC (European Union, 1995)

Registries cross a number of legal boundaries as they lie at the intersection between four key areas of law - public health, women's rights, medical research, and information law (including data protection law and increasingly, the right to health and privacy). There are a number of legal instruments with international significance and the spirit of the law. In some cases, the letter of the law has been implemented into national laws.

The European Directive 95/46/EC has been instrumental in helping to make data protection policies more uniform across the world. The driving force of the Directive's impact is that it requires that there are equivalent standards of data protection if data is sent to another country. This means that countries have adopted these standards when drafting their own legislation. Currently under review, new forthcoming regulations are being drafted that will replace this Directive.

The norm in most countries is that there is not specific national legislation to cover registries. One country that does this differently is Norway that has specific legislation as well as specific guidelines that cover many of the national registries. In most countries, however, there is legislation that covers the collection of births, deaths and marriages, as well as specific legislation for census collection and in some cases statistical research. Registry activities will also fall under more general law, such as data protection or law that allows the use of medical records for health purposes. An example of this is the UK, where a specialist body, HRA Confidentiality Advisory Group, approves the uses of identifiable information by registries, on a case by case basis so that collection of data without consent must be justified.

These examples suggest that many different approaches can and do work. Stakeholder involvement and public engagement, however, are integral to the success of any strategy.

4.3 OVERSIGHT

Depending on a country's organizational health structure or legislative foundation, it may be advisable to seek formal oversight by national regulatory bodies so that an eRegistry provides additional transparency to the general public. Two regulatory bodies that are particularly relevant to registry operations include national ethical review bodies and data protection authority bodies. A third consideration would be to involve an existing financial auditing authority to provide fiscal oversight.

4.3.I ETHICAL OVERSIGHT

In most countries, a national ethical review board or committee can be identified to provide ethical guidance and oversight for research involving registries or other ethical matters. Given the diversity of ethical and legal requirements throughout the world, it is advisable to consult legal counsel in your country to determine whether a formal ethical approval process is necessary. Similarly, in some settings, it may be advisable to seek and obtain approval from a national authority such as a Research Ethics Committee (REC) or a formal approval for exemption of obtaining informed consent.

Secondly, an eRegistry should have access to an ethical review board or committee if there is any intention of granting researchers access to eRegistry data. Although non-confidential data may be publicly available to any researcher, confidential data must involve an application process with strict qualifications (see also Section 5.5 Data Access and 5.7 Templates) and involve an approval process by an external ethical review committee or board that will evaluate the research/researcher.

4.3.2 DATA PROTECTION OVERSIGHT

The eRegistry may wish to identify an oversight body that assumes responsibility for national data protection, i.e., Data Protection Authority agency or board. Data protection authority bodies or data safety monitoring boards can provide expertise, advice, and oversight concerning data security issues. (See Resources under section 5.I, Data privacy legislation for a comprehensive list of data protection authority bodies in existence worldwide.)

If a national data protection authority with the capability to monitor specific registries is not viable, an alternative approach is to appoint a Personal Data Protection Official. Article I8, section 2 of the EU Directive 95/46/EC articulates the possibility that a controller may appoint an official if it is provided for in the Member state's legislation. The forthcoming EU Directive on data protection also recognizes this option of appointing a 'privacy ombudsman,' as it is referred to in Norway.

NORWAY: AN EXAMPLE OF BOTH LAW AND GUIDELINES GOVERNING REGISTRIES

legislation

The recently issued Norwegian Health Registry Act (helseregisterloven) (2014), effective as of January 2015, mandates and governs a series of registries including a cause of death registry, medical birth registry, cancer registry, prescription registry and a Norwegian patient registry.

guidelines

The Norwegian Institute of Public Health Guidelines on Delivery of data from central personal health data filing systems govern who can access identifiable data and in what circumstances (e.g. researchers with ethics approval). There are also guidelines for specific registries such as the Guidelines for access to data from the Norwegian Prescription Database that requires projects to be evaluated as legitimate and justifiable before being granted access to data.

05 - governance

There are many definitions of governance and regulation; narrow and broad. In its broadest sense, governance can be described as 'the intentional activity of attempting to control, order or influence the behavior of others[71] and, therefore, can cover multiple actors, activities and mechanisms. It can be distinguished from regulation that is narrower in scope and applies to the formal structures of law and legal bodies.

Governance can be carried out through a number of different mechanisms such as documents, procedures, people and professional values and culture. Legislation, regulations, professional guidance and policies, for example, can guide and sometimes dictate behavior.[72] Procedures can then be put in place that support the governance documents and can consist of informal, implicit, institutional norms or 'the way we do things,' as well as more formal procedures that maybe required by law or regulatory bodies (such as licenses and applications for access).

Values and culture that are implicit in a particular context may also influence the way that these various elements of governance are enacted.[72] The current aim is to develop flexible, responsive governance structures that are able to adapt and respond to ethical, legal and social challenges over time.[73]

The benefit of governance is that it promotes certainty and efficiency as people know what the rules are, what happens, and when. It can ensure uniformity and equality— that things are done in a uniform way with everyone and the same issues are being treated the same. This system means problems can be anticipated as there are mechanisms to deal with the routine issues but anticipated situations can also be resolved efficiently. Having a governance system in place ensures that ethical and lawful research is supported through accountable and transparent decision making that will promote public confidence and trust.

An effective governance system embodies the better regulation principles of proportionality, accountability, consistency, transparency and targeting outlined by the Better Regulation Task Force (2007). These principles, therefore, require that oversight mechanisms are coherent, appropriate and efficient, and that there are clear lines of accountability for regulators.

5.1 GOVERNANCE PLAN

This section must outline the fundamental elements for a registry governance plan. Each country or setting will need to customize this plan according to their own unique objectives and working within parameters of their country's overall organizational health structures.

Good governance is crucial even if there is legislation or formal regulations, as it provides the procedures to enable the registry to function but also for effective reporting and compliance. A reproductive health registry should be anchored in a legal framework, just as in a civil registration.[74] In settings that lack strong infrastructure or regulations, robust governance provided through informal mechanisms such as guidelines, procedures, and policies will help to safeguard the integrity of the registry.[75]

As mentioned previously, a number of fundamental components are vital to the functioning of a registry and should be addressed and documented in the registry's governance plan. Given the importance of encouraging active change development of the governance framework, revision management has been added to this list.

To reiterate, these focal topics include:

1. Purpose of the registry
2. Legal, fiscal, and operational responsibility
3. Reporting requirements, compliance, and enforceability
4. Data quality and standards
5. Data security, confidentiality, and access
6. Public engagement[43]
7. Revision management

5.2 REGISTRY DOCUMENTATION

All elements of the registry's governance plan should be written in a document or set of documents. The documentation should summarize the purpose, goals, objectives and structure of the organization and be publicly available (i.e., on a website). This will go some way towards maximizing transparency and gaining public trust.

Written documentation on the registry's governance is important for efficient operations. These may comprise of bylaws, administrative manuals, or standard operating procedures (SOPs). Additional documentation concerning data collection may include manuals on data definitions, data collection protocols, inclusion/exclusion definitions, data entry

procedures, analysis protocols, hardware and software manuals, security and confidentiality policies and data access policies.[17] The responsibility of developing and implementing guidelines and data collection protocols should be a joint venture by the Board and the Ministry of Health or other body.

5.2.1 PURPOSE

EXAMPLE OF STATEMENT OF PURPOSE

The purpose of an eRegistry for maternal and child health is to provide reproductive, maternal, newborn, and child health (RMNCH) data that can be used for public health surveillance, public health planning, priority setting, and quality of care and service delivery.

eRegistry data will be used to monitor the continuity and coverage of RMNCH care. In the case of the secondary use of registry data for the purpose of RMNCH research, eRegistry data will only disseminated on an aggregate level.

eRegistry data provided to public health officials, health care providers, and participating women is intended to improve program and policy planning, clinical decision-making, and quality of care.

The purpose and scope of the eRegistry with regard to public health surveillance on reproductive, maternal, newborn, and child health (RMNCH) data should be clearly defined. Registry operations should be delineated in the statement of purpose in order to provide strategic, administrative, and managerial direction and focus. From a legal perspective, if the registry's activities were questioned or challenged, the registry statement of purpose should provide legal clarity. Primary and secondary aims may be stated under the purpose statement, with a description of the health system outcomes that the registry will enable or support, and a statement of the benefits to stakeholders.

5.2.2 AUTHORITY

An appropriate state body or agency must authorize the Registry to implement and maintain an RMNCH database, assume legal and fiscal responsibility for the Registry and be accountable to the public for all Registry-related issues. Institutional affiliations and partnerships with the Registry should explicitly assign roles and responsibilities. Jurisdiction (i.e. geographic sphere), management and administrative organization and responsibilities should be clearly defined. An organizational chart of these relationships may add further

EXAMPLE OF STATEMENT ON LEGAL AUTHORITY

The eRegistry operates under the jurisdiction of the [insert Ministry of Health or other legal authority] and will partner with [Insert National Institute of Public Health or other designated affiliation] in the geographic area of [insert country/geographic location].

clarity in defining authority, roles, and responsibilities.

5.2.3 CUSTODIANSHIP

The concept of ownership does not fit health information comfortably, because it largely fails to acknowledge individual patient privacy interests in health information... The legal concept of custody may be a useful alternative to that of ownership.[55]

EXAMPLE OF STATEMENT ON CUSTODIANSHIP

The eRegistry's Custodian, [Insert National or state body] will assume legal, financial, and strategic responsibility for the Registry.

eRegistry staff and registry sources (i.e., persons, providers, or institutions) reporting health information to the Registry as per protocol will not be liable in any legal proceedings for such actions.

The reproductive health registry is affiliated with the [Insert Body] and partners with [Insert Body].

Custodianship (as opposed to ownership) is an acceptable legal approach for describing registry data. In terms of the Registry's custodianship, the issue of liability should be addressed to relieve Registry staff and sources from all legal liability or civil action for eRegistry activities that are conducted in compliance with standard operating procedures and policies.

Registry staff found to be not in compliance with policies regarding privacy and confidentiality, conversely, may be subject to disciplinary action and/or dismissal/termination from employment.

5.2.4 ACCOUNTABILITY

Regular reporting to the eRegistry's affiliates, partners, and constituents assures the public accountability. Routine reporting to the Ministry of Health and Department of Health and governance bodies (i.e., Registry management Board, Advisory board) should occur. Regular reporting to a Data Protection Authority or information governance body provides accountability to data security issues.

All staff members should be clear about their responsibilities in regard to the data that is being held in the registry and should be provided with appropriate training. Publicly available reports produced by the eRegistry must demonstrate transparency and instill public trust.

A communication plan describing how the registry will disseminate information to their range of stakeholders will

ensure that data are used by public health officials, health care providers, and women and their families. Non-compliance with the law and policies of the eRegistry should be dealt with promptly and appropriately, and the activities of the eRegistry should be reviewable by a court of law.

5.2.5 PUBLIC ENGAGEMENT

Engaging all stakeholders as well as the public sector is essential to the success of an eRegistry.[75] Establishing a protocol to maintain public engagement through routine communication (i.e., a regularly updated website with information) will instill trust and encourage support among the general public and the eRegistry's stakeholders. Monitoring public opinion with the regard to the eRegistry is also important.[76] Public engagement campaigns may strengthen public trust and facilitate eRegistry activities.

5.2.6 DISSEMINATION

Dissemination is fundamental to fulfilling a primary goal of the eRegistry- that of improving the health of women and children. Given that a fundamental tenet of an eRegistries framework is to demonstrate the value of registry maximize its use by all stakeholders by packaging and publishing registry data in usable formats. Consistent report distribution to constituents is a vital function performed by the eRegistry that should facilitate performance evaluation, resource allocation, and public health decision making. Standards should be documented regarding frequency, format, audience, and dissemination channel to ensure that stakeholders receive timely and useful information.

Established routines for producing and sharing annual reports should be documented. Report content may include summary registry data by year, region, district, facility, or other divisions and distributed electronically or in hard copy each year to facilities, legislators, and other registry liaisons. Reports to facilities and/or special reports, upon request, should be processed regularly

EXAMPLE OF STATEMENT ON DISSEMINATION

The registry will compile, generate, and disseminate publicly available annual reports, summary reports to registry sources, and produce ad hoc reports as requested.

In the case of the reporting of aggregate data, confidentiality policies should be in place to prevent the inadvertent identification of individuals due to small sample sizes. The registry may decide to withhold publication of tables with less than a predefined number of individuals or rely on the denominator to determine the suitabiliyt of reporting statistics.

by the eRegistry. Timeliness should be an explicit goal.

It is advisable to develop standards on data presentation, source information, statistical methods and analysis, interpretation of results, and clear explanations of graphs, tables, or other graphical displays of data. In particular, to further protect individuals' privacy, it is advisable to institute a protocol that prohibits the publication of small cell sizes or tables with few data points to prevent any possibility of individuals' identities being compromised. In sum, the value of an eRegistry may be calculated by the extent to which data is analyzed and disseminated to relevant audiences. Unused data or underutilized reporting significantly diminishes the intended value of a registry.

EXAMPLE: STATEMENT ON THE EREGISTRY MANAGEMENT PRESIDENT/BOARD/COMMITTEE

1. To oversee the eRegistry's management, organization, and development
2. To maintain fiscal responsibility of the eRegistry
3. To assess the mission and strategic direction of the eRegistry
4. To review eRegistry 's compliance with health, data, and privacy legislation
5. To advise on data collection, cleaning, and analysis processes
6. To review reports and data published by the eRegistry
7. To develop and monitor policies for data access
8. To create a communication strategy with stakeholders and the public
9. To assess and address stakeholders' interests
10. To encourage public engagement and open dialogue

5.3 GOVERNANCE STRUCTURE

5.3.1 MANAGEMENT BOARD

A director, board, committee, or other governing body responsible for the operations and activities of the eRegistry, may also govern management of the registry's routine operations. The authorized person or institution may depend on a country's definition of a legal entity or body.

Roles and responsibilities of this 'body' may include the following:

- Oversee the eRegistry's management, organization, development
- Maintain fiscal responsibility and ensure funding for the eRegistry
- Advise on the mission and strategic direction of the eRegistry
- Review the eRegistry's compliance with data privacy legislation
- Advise on data collection,

cleaning, and analysis processes
- Review reports and data published by the eRegistry
- Develop and monitor policies for data access
- Create a communication strategy with stakeholders and general public
- Consider all stakeholders' interests (i.e., public health officials, public health community, health care providers, researchers, women and families)
- Encourage public engagement and open dialogue

5.3.2 ADVISORY BOARD

Independent advisory boards may provide external oversight to the eRegistry and assist in providing guidance on technical or scientific aspects of the eRegistry.

EXAMPLE OF STATEMENT ON ADVISORY BOARD

The role of the Advisory Board is to provide long term strategic advice for the eRegistry and to provide external advice and training opportunities for the eRegistry.

The eRegistry Advisory Board will include members representing multidisciplinary fields such as reproductive health, epidemiology, health information systems, public health, biostatistics, law, ethics, and the lay public.

Members of an advisory board may include members from the medical fields (i.e., obstetricians, gynecologists, general practitioners, midwives, nurses, and community health workers), the scientific/academic community (i.e., researchers, public health officials, epidemiologists, and statisticians), law (i.e., legal and ethical advisors) and the general public.

5.3.3 EXTERNAL EXPERTS

External consultants or experts in the field of reproductive public health, medicine, law, or ethics may be useful in advising the eRegistry on scientific or legal matters. Interactions with related government agencies, universities, or private organizations may also be helpful in assisting or supporting the eRegistry through consulting or for training purposes.

5.3.4 STAKEHOLDERS

Consultations with stakeholders to gather input and ensure they are involved for duration of the program via reference groups, engagement forums, public consultations, and communication strategy and plans is integral throughout all phases.

06 - registry data

6.1 CONSENT

Health registries with legal mandates and authority to collect or receive information for the purpose of public health surveillance often do not require individual consent or refusal.[77] The justification for implied consent is that public health surveillance data is in the public interest and deemed a 'public good' that can be counterbalanced by strict confidentiality protocols protecting individuals' privacy. Therefore, if implied consent policy is chosen, broader governance may be an appropriate strategy to compensate for this situation.

In some circumstances, consent options used by some registries include opt-in, opt-out, broad, or standard informed consent.[61] A distinct disadvantage of these consent options, however, is that they result in significantly decreased participation which can de-value the overall objective of the registry - to obtain population-based data to improve the overall health of a society.[78] Requiring informed consent from participants may seriously impact the validity and undermine the integrity of the registry as those who do not provide consent may differ from those that provide consent. This area has attracted a great deal of media attention and discussion among researchers given that requiring consent has resulted in dramatic declines in registry enrollment.[60,78-81] Public engagement and full disclosure on why and how data is collected can help acquire and maintain support for the registry's chosen consent protocol.[77] The right to withdraw, however, should be ensured and provided under law.

As a corollary, secondary use of registry data for research purposes is not considered essential to the 'public good' and, therefore, is not exempt from informed consent requirements. Legislation in Norway, for example, provides participants the opportunity to opt out of allowing their data to be used for research purposes. Many other countries also stipulate that patient consent is necessary before registry data can be used for research purposes.

6.2 DATA PRIVACY (OR PROTECTION) LAW

The eRegistry must be compliant with data protection, privacy legislation or regulations at all times. Data collection, storage, and transmission of data must adhere to all legislation concerning health data or information, electronic personal data, data

privacy, and/or data sharing. Moreover, the eRegistry must monitor legislative changes to assure compliance of law(s) at all times.

The recent development of information communication technologies has resulted in a great deal of attention towards data privacy.[33,82-87] Although there are significant differences regarding the cultural interpretation of personal privacy, there is some universal consensus. According to Privacy International, for example, the vast majority of developing countries' constitutions explicitly refer to the notion that national policies should not interfere with their citizenry's privacy.[88]

Likewise, the World Health Organization's 2nd global survey on eHealth reports that, although many countries have not yet adopted data privacy or protection legislation, nearly all countries acknowledge the importance of personal privacy.[89] Thus, although historically health information privacy protection embedded in professional codes of conduct was considered adequate, technological advances have demanded additional safeguards.[89]

The field of data privacy law has, and continues, to experience dramatic growth. Despite variations in content, more than 100 countries worldwide have enacted some sort of data privacy statutes and this number is expected to increase in the coming years.[66] As one might expect, the research and analysis of data privacy and security laws has tended to focus on developed countries.[90] That said, impressive progress in numerous French-speaking African countries has been achieved as a result of support provided by the Association of Francophone Data Protection Authorities.[91]

Despite noted variation in content and scope, a report prepared by Policy Engagement Network[39] observed four common principles:

- respecting self-determination
- collection and management
- access and disclosure
- monitoring compliance and accountability

The first principle, respecting self-determination, concerns the rights of individuals to withdraw or access their own data. Second, collection and management focuses on the obligations of ensuring data security and confidentiality. Third, access and disclosure limits or regulates access to individual data by third parties or for secondary use. And, finally, monitoring compliance and accountability addresses issues concerning registry liability and how security breach notifications are handled.

DATA PRIVACY LAW RESOURCES

1. **DATA PRIVACY LAWS: AN INTERNATIONAL PERSPECTIVE (2014)**
   a book authored by L.A. Bygrave[66] offers a comprehensive analysis of data privacy law around the world with compelling insight regarding future directions.

2. **GLOBAL TABLES OF DATA PRIVACY LAWS AND BILLS (3rd edition, September 2013)**
   compiled by Graham Greenleaf[67] can be accessed here: **http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2280875**.

3. **MHEALTH REGULATION IMPACT ASSESSMENT: AFRICA by GSMA**
   provides a summary of the legal and regulatory landscapes concerning privacy and data protection in ten sub-saharan african countries. The full report can be accessed here: **http://www.gsma.com/mobilefordevelopment/mhealth-regulation-impact-assessment-africa**

4. **DATA PROTECTION LAWS OF THE WORLD, THIRD EDITION by DLA Piper (January 2014)**
   an online handbook with an overview of data protection laws in more than 70 jurisdictions that is available here: **https://www.dlapiper.com/en/global/insights/publications/2014/01/data-protection-laws-of-the-world-handbook/**

5. **2014 INTERNATIONAL COMPENDIUM OF DATA PRIVACY LAWS, compiled by Baker and Hostetler**
   can be accessed here: **http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/International-Compendium-of-Data-Privacy-Laws.pdf**.

6. **Norton Rose Fulbright has assembled a directory of global data privacy laws**
   can be accessed here: **http://www.nortonrosefulbright.com/files/global-data-privacy-directory-52687.pdf**.

6.3 DATA SECURITY

> *It is well established in the field of information security that the greatest threats to an organization's information assets come from within (pg. 16).* [39]

Due to the highly sensitive nature of reproductive health data, it is critical for the eRegistry to implement and enforce strict data security and confidentiality policies.[39,90,92-94]

Reproductive health data may include pregnancy history, HIV status and abortion procedures, any of which could be considered stigmatizing or compromising for individuals in some settings if privacy is not rigorously maintained.

Protecting the confidentiality of individuals and reporting sources is a fundamental ethical obligation of the eRegistry. If the general public does not have full confidence in the eRegistry's ability to maintain privacy and confidentiality, individuals may attempt to avoid inclusion. The eRegistry should clearly stipulate who is responsible so that there is transparent ownership of the process.

Working under the umbrella of the DHIS 2 platform, the eRegistry's data security is naturally predicated on the security protocols and policies provided in the DHIS software such as administrative procedures such as passwords, user authentication, and user role-based access.

The eRegistry's data security plan may also address the following:

- Physical security such as alarms, locks, or security guards

- Technical security protocols such as internal and/or external firewalls, routine virus checking and antivirus software, security breach protocols and noncompliance policies, encryption and defined/limited access to linked data files, data storage, backup, and recovery policies.

- A written data security policy document (i.e., security manual) to facilitate training, adherence, and auditing procedures. The security policy manual should be available to all registry staff, used in training, regularly updated and evaluated. The security manual should address physical, administrative, and technical safeguards (as mentioned above) and as well as consequences of noncompliance that may include corrective disciplinary action, reduced access to data, retraining, or termination

of employment, if warranted.

- Employment contracts should include clauses regarding data privacy and confidentiality, compliance and consequences.

A coherent security strategy must also be adaptable and acknowledge the ever-changing threats and risks that confront the registry.

The way in which eRegistry data is formatted and handled can also help address personal privacy and protect confidentiality. De-identification (or anonymization), for example, removes all identifiers (e.g., name, email, address, etc.) so that information cannot be linked to a specific individual.[94]

Pseudonymization, on the other hand, replaces data elements with new identifiers so that the data appears complete and the context is preserved while maintaining patient privacy. Pseudonymized data can be re-identified which therefore maintains the integrity of the original data set. A strategy known as 'privacy by design' is a growing field that asserts that security measures should be fully embedded in all aspects of data architecture and design from an early stage.[95]

In addition, a review of security and privacy strategies in the mHealth field resulted in a minimum set of recommended requirements that include the following nine properties: access control, authentication, security and confidentiality, integrity, patient information, data transfer, data retention, BANs communication, and breach notification.[90]

The confidentiality of eRegistry data follows similar standards of privacy adhered to in the historic patient-provider code of honor. The need for more formalized protocols, however, reflects the shift in the potential of health data to be inadvertently or expressly accessed or shared in a digital world. To address these concerns, a written confidentiality policy for registry participant data should address the following:

- Employee staff confidentiality agreements
- Policy preventing the release of confidential information from the Registry for any legal proceedings
- Policy and procedures concerning confidentiality breaches
- Policy on eRegistry participants' access to data (i.e. corrections, etc.)
- Limitations on releasing aggregate data that has potential to indirectly reveal individual identities

It is also important to note that although hacking is perceived to pose the greatest threat, internal system malfunctions and human error are often responsible for many privacy violations. Thus, it is important to consider how to mitigate internal threats by implementing computer training and education to create a strong culture of data privacy. Technological safeguards are necessary, but insufficient, in ensuring data security.

Finally, compliance and enforcement are essential to data security policy. Consequences for intentional or unintentional misuses of data should be clarified. Lack of enforcement, sanctions, disciplinary action or other remedies for disclosure, reduces the overall confidence in the registry and enforceability becomes compromised.

EXAMPLE OF EREGISTRY DATA SECURITY POLICY

The eRegistry will safeguard data by taking the necessary administrative, technical, and physical security measures (i.e., password protection, encryption, firewalls, virus protection, etc.) to ensure the highest level of data security at all times. Enforcement of security standards, ongoing training, and protocols for security breaches and penalties for violations must be specified.

Example of eRegistry Confidentiality Policy: The eRegistry's confidentiality policy is intended to protect individually identifiable data and should involve a written protocol on practices that address all sequential Registry data processing phases and their consequent vulnerability. The policy should specify the confidentiality of Registry data that would prohibit the disclosure or release for any legal proceeding.

6.4 DATA REPORTING

EXAMPLE OF EREGISTRY REPORTING

The eRegistry aims to collect population-based RMNCH data in the [jurisdiction]. Reporting by [indicate all relevant health providers] is required to report RMNCH data to the central Registry within [state time frame] and adhere to the definitions contained in the eRegistry's data dictionary.

The success of the eRegistry depends on the completeness, timeliness and quality of its data.[43] To be representative, the eRegistry must be population-based. It is, therefore, important to have a national directive that states that reporting to the eRegistry by health care providers and facilities is compulsory.

Typically, an effective directive that requires health providers to report health information to a registry database is grounded in legislation or in guidelines. These should specify who, when, and how data is provided. Consequences or penalties for noncompliance or delayed reporting may also be mentioned.

6.5 DATA QUALITY

Data quality is essential to the success of an eRegistry. If the quality of the data is inconsistent, delayed, or unreliable, those involved may lose confidence and the validity of the data may be questioned. The daily operation and maintenance of an eRegistry, therefore, depends on formalized and documented data procedure protocols that clearly delineate coding procedures, data elements, a data dictionary, and quality assurance procedures during and after data capture.[43]

The eRegistry must have a data manual that is available to staff for training and review. Written procedures and protocols addressing data quality issues throughout data collection, data entry, and final data cleaning should be continually evaluated. Quality assurance procedures at all data capture points should be analyzed for potential error. Finally, a set of diagnostics should investigate suspicious data entry patterns, missing data clusters, and other threats to validity.

EXAMPLE OF DATA QUALITY STANDARDS

Routine measures following written protocols will address how to ensure completeness, accuracy, and overall quality of data. Strategies to identify incomplete or inaccurate data throughout the data capture/entry/analysis continuum will be developed and implemented in order to improve data completeness and accuracy.

6.6 DATA ACCESS

> ***Establishing a policy for data access is a crucial task in the development of a registry. When data are requested, registry administrators will have to respond. It is far superior to have a fair and effective policy for determining how to handle such requests rather than handling them on an ad hoc basis. If requests are ignored, side-tracked or arbitrarily rejected, a lawsuit could ensure and access to the data will be determined by the courts. (pg. 150)*** [17]

Data access policies regarding eRegistry data should be carefully planned and documented in order to maintain participants' privacy and confidentiality. The value and importance of analyzing, sharing and using eRegistry data to advance public health, however, should also be recognized as an integral objective of the eRegistry. Aggregate eRegistry data can, for example, be used to its fullest potential while still ensuring individuals' privacy since health data in aggregate form is not considered sensitive personal information.

Access issues will vary according to internal versus external outside sources seeking access and will differ based on the type of data requested (i.e., aggregate, anonymized, etc.). Internal policies regarding registry publications, authorship, or scientific presentations should be delineated in a written policy.

Internal data sharing policies between facilities also needs to be addressed. There is significant variation across countries in how this issue is managed. Despite the potential benefits to patients for facilitating data sharing, privacy issues can hinder this potential.

In sum, issues that need to be addressed include:

- Who has access to registry data?*
- What kind of registry data can they access (i.e., de-identified, anonymized, etc.)?
- How can they access data?
- What are the obligations and conditions that concern data access and use?
- Is it free or is there a cost? Is the cost the same for everyone?

Given that health data collected for a registry is conducted for the public common good, access policies should follow a transparent approach.

To maintain an optimal balance between protecting the privacy and confidentiality of individual health data while supporting research efforts using data, the eRegistry must enforce strict guidelines before releasing data to researchers. The declared purpose of the research should correspond closely with eRegistry regulations and must be evaluated as

legitimate and justifiable from an ethical perspective.

Forms, application procedures, and policies should be formalized to guarantee maximum data security. Section 5.7 provides a list of suggested data access forms and/or templates. A flowchart may be useful in outlining the steps taken when registry data is requested by researchers. Internal and external requests, for example, will adhere to different procedural protocols.

EXAMPLE STATEMENT ON DATA ACCESS POLICY

To facilitate access to eRegistry data, non-confidential registry data files may be available for with restricted access or for general public use. A policy describing how to access registry data will be developed and available to scientific investigators and/or academic researchers will insure public access to anonymized, aggregate registry data. Data analysis and dissemination with appropriate data privacy measures in place is consistent with the eRegistry's purpose and also enhances overall value.

Typically, requests to access eRegistry data involve an external Institutional Review Board (REC) approval process. The format of the data that is requested will impact the type of the ethical approval required. If the data requested is anonymized or de-identified, a waiver of ethical approval is commonplace. Otherwise, consent from eRegistry participants may be required. The secondary use of eRegistry data is usually considered subject to consent with the explicit option available to all participants to opt-out if desired.[77] Individually identifiable information is typically not provided to investigators without participant consent.

Researchers that are provided access to registry data also incur responsibilities and obligations to safely and appropriately dispose of registry data after use. Other issues to consider include how long data can be kept, whether data is deleted, stored, returned to the registry, or deposited with a trusted third party are also important considerations.

Finally, patient access to their individual data should be addressed. Access to data and data ownership are two inextricably linked concepts so there should be conformity in how these issues are addressed. From an ethical perspective, each individual 'owns' their personal health information and, therefore, their personal health data contained in the registry. From a data quality standpoint, patients have a vested interest in insuring that their health information is correct so allowing access would have a secondary benefit of enhancing the

registry's data quality.

Moreover, participants should not be expected to endure incorrect, incomplete, or mistaken personal health information to persist in the registry. Making changes and/or deletions in patient records (which may be hidden or not) should be clarified in eRegistry documentation. A determination of whether data access is free or has financial costs associated with it should also be noted.

6.7 AUDIT POLICY

Routine auditing of data collection processes, quality assurance of data, adherence to security and confidentiality policies and data access policies should be performed periodically. In particular, a thorough risk assessment of the eRegistry is advisable given the highly sensitive nature of reproductive health rights and privacy.

EXAMPLE STATEMENT ON AUDIT POLICY

The eRegistry will monitor and evaluate all internal and external registry activities concerning data collection, maintenance, security, and storage. An audit trail (e.g., activity logging) documenting data access according to person, place, and purpose will be implemented. Assessment and management of risks, especially concerning data security and confidentiality, must be routine practices. Compliance with policies, regulations, and laws will also be prioritized.

6.8 DOCUMENTATION

There are numerous templates that can be developed to document the procedures of sharing or releasing eRegistry data to external researchers. The following is a list of key documents describing policies, protocols, procedures, and agreements for monitoring and tracking eRegistry data.

DOCUMENT	DESCRIPTION
data request flowchart	a flowchart will map the decision-making processes of data requests
data release protocols	when, to whom, under what circumstances and what kind of data should be released
data access guidelines	the criteria used to determine whether access will be granted to interested researchers or institutions needs to be included in guidelines
data access applications	the review and approval process should entail an application that requests information on the principal investigator, the proposed research project, the research methodology, the timeline and duration, and the security and confidentiality protocols that will be in place to protect eRegistry data
data sharing contracts	data exchange agreements outlining the parameters of the acceptable data use
data security contracts	agreements that outline compliance with security issues when using eRegistry data
publication process	description of authorship protocols and required acknowledgements

Additional policy documents that may be developed include:

DOCUMENT	DESCRIPTION
privacy policy	staff practices and procedures to ensure data privacy
breach management	processes concerning reporting, containing, notifying, investigating and remediating privacy breaches
data storage/destruction	procedures for storing and destroying data after use
information security	strategy outlining physical, technical, and administrative measures that ensure confidentiality, and integrity of registry data
data sharing agreement	description of stipulations on how data will be shared by different facilities
confidentiality agreement	employee signed statements ensuring compliance with privacy and security policies

6.9 REGISTRY TERMINATION

The intention of the eRegistry is to continue to operate contingent on proper management and sufficient funding. In the event that the eRegistry terminates operations, de-identified data will be stored on an encrypted digital storage device and returned to the eRegistry authority for safekeeping. eRegistry data will be stored for a minimum of thirty years.

appendix I summary of eRegistries documentation

Statement of Purpose

The purpose of the eRegistry for maternal and child health is to provide reproductive, maternal, newborn, and child health (RMNCH) data that can be used for public health surveillance, public health planning and priority setting, and quality of care and service delivery.

eRegistry data will be used to monitor the continuity and coverage of RMNCH care. In the case of the secondary use of eRegistry data for the purpose of RMNCH research, eRegistry data will only disseminated on an aggregate level.

eRegistry data provided to public health officials, health care providers, and participating women is intended to improve decision making, policy planning, clinical decision-making, and quality of care.

Statement of Authority

The eRegistry operates under the jurisdiction of the [insert Ministry of Health or other affiliation] and will partner with [Insert National Institute of Public Health or other designated partnership] in the geographic area of [insert country/geographic location].

Statement of Custodianship

The eRegistry's Custodian, [Insert National or state body] will assume legal, financial, and strategic responsibility for the eRegistry.

eRegistry staff and registry sources (i.e., persons, providers, or institutions) will not be held liable for reporting health information to the eRegistry.

Statement on the Board

1. To oversee the eRegistry's management, organization, and development
2. To maintain fiscal responsibility of the eRegistry
3. To assess the mission and strategic direction of the eRegistry
4. To review the eRegistry's compliance with health registry, data, and privacy legislation
5. To advise on data collection, cleaning, and analysis processes
6. To review reports and data published by the eRegistry
7. To develop and moniwtor policies for data access
8. To create a communication strategy with stakeholders and the general public
9. To assess and address stakeholders' interests
10. To encourage public engagement and open dialogue

Statement on Advisory board

The role of the Advisory Board is to provide long term strategic advice for the eRegistry and to provide external advice and training opportunities for the eRegistry.

The eRegistry Advisory Board includes members from multidisciplinary fields including reproductive health, epidemiology, health information systems, biostatistics, law, ethics, and public health.

Statement on Data security

The eRegistry will safeguard data by taking the necessary administrative, technical, and physical security measures (i.e., password protection, encryption, firewalls, virus protection, etc.) to ensure the highest level of data security at all times. Enforcement of security standards, ongoing training, and protocols for security breaches and penalties for violations must be specified.

Statement on Confidentiality

A policy intended to protect individually identifiable Registry data should involve a written protocol on practices that address all sequential eRegistry data processes that have been identified as potentially vulnerable. The policy should specify the confidentiality of Registry data that would prohibit the disclosure or release for any legal proceeding.

Statement on Data Quality

Routine measures following written protocols will address how to ensure completeness, accuracy, and overall quality of eRegistry data.

Strategies to identify incomplete or inaccurate data throughout the data capture/entry/analysis continuum will be developed and implemented in order to improve data completeness and accuracy.

Statement on Data Access

To facilitate access to eRegistry data, non-confidential data files may be available for with restricted access or for general public use. A policy describing how to access registry data will be developed and available to scientific investigators and/or academic researchers will insure public access to anonymized, aggregate data. Data analysis and dissemination with appropriate data privacy measures in place is consistent with the eRegistry's purpose and also enhances overall value.

Statement on Auditing

The eRegistry will monitor and evaluate all internal and external registry activities concerning data collection, maintenance, security, and storage. An audit trail (e.g., activity logging) documenting data access according to person, place, and purpose will be implemented. Assessment and management of risks, especially concerning data security and confidentiality, must be routine practices. Compliance with policies, regulations, and laws will also be prioritized.

Statement on Dissemination

The eRegistry will compile, generate, and disseminate publicly available annual reports, summary reports to eRegistry sources, and produce ad hoc reports as requested.

In the case of the reporting of aggregate data, confidentiality policies will prevent the inadvertent identification of individuals due to small sample sizes. The eRegistry will withhold publication of tables with less than a predefined number of individuals or rely on the denominator to determine the suitability of reporting statistics.

appendix 2 interational instruments

In the absence of national legislation or regulations, international conventions, guidelines and/or declarations may offer a useful starting point given their focus on fundamental human rights, privacy, and/or data security.

This appendix presents a list of relevant international instruments, declarations, and treaties that may be relevant to eRegistries and briefly describes their content and significance.

MEDICAL RESEARCH INVOLVING HUMAN SUBJECTS

The World Medical Association Declaration of Helsinki: (http://www.wma.net/en/30publications/10policies/b3/) asserts that an essential human right is that medical and personal data are treated as confidential with two exceptions: l. disclosure would prevent serious harm to public health or, 2. for use in a criminal case in a court of law.

HUMAN RIGHTS AND THE RIGHT TO PRIVACY

The following two documents represent two of the most important covenants on human rights. They are legal binding through ratification or accession.

UN Covenant on Civil and Political Rights with additional protocols: http://www.ohchr.org/EN/ProfessionalInterest/Pages/OPCCPRI.aspx

United Nations Covenant on Economic, Social and Cultural Rights: http://www.ohchr.org/EN/ProfessionalInterest/Pages/CESCR.aspx

Universal Declaration of Human Rights: http://www.un.org/en/documents/udhr/

Universal Declaration on the Human Genome and Human Rights (1997): http://wwwl.umn.edu/humanrts/instree/Udhrhg.htm

Resolution on Human Rights and Bioethics: http://www.unhchr.ch/Huridocda/Huridoca.nsf/0/d85deea99805ebf68025676600491l00?Opendocument

Operational Guidelines for Ethics Committees that Review Biomedical Research: http://whqlibdoc.who.int/publications/20ll/978924l502948_eng.pdf

International Ethical Guidelines for Biomedical Research Involving Human Subjects: http://www.cioms.ch/publications/layout_guide2002.pdf

European Convention on Human Rights Act 2003: http://conventions.coe.int/Treaty/en/Treaties/Html/009.htm

Convention on Human Rights and Biomedicine: http://www.humanrights.ch/en/Standards/CE-Treaties/Biomedicine/index.html

The Belmont Report: http://hhs.gov/ohrp/humansubjects/guidance/belmont.htm

DATA PROTECTION

EU Data Protection Directive (1995/46/EF Directive) on the processing and exchange of personal data: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:3l995L0046:en:HTML

EU Data Protection Directive, also known as Directive 95/46/EC, was designed to protect the privacy and protection of all personal data collected for, or about, citizens of the EU, especially concerning the processing, use or exchange of data. Directive 95/46/EC encompasses all key elements from Article 8 of the European Convention on Human Rights that states its intention to respect the rights of privacy in personal and family life, as well as in the home and in personal correspondence. The Directive is based on the 1980 OECD "Recommendations of the Council concerning guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data."

OECD Guidelines on Data Protection: http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

The OECD Guidelines are based on fundamental privacy principles including data purpose specification, openness, individual participation, collection limitation, data quality, use limitation, data security safeguards, and accountability. Although originally published in 1980, these guidelines were recently revised in September 2013. The revisions address the importance of national privacy strategies, privacy management programs, and data security breach notification. Privacy enforcement with regard to international data flow and risk assessment has been added as well.

PRIVACY – REGIONAL LEVEL

A large majority of countries have provisions in their constitutions ensuring that national policies do not interfere with an individual's privacy.[88] Other documents address the issue of privacy on a regional level as in the examples mentioned below.

African Charter on Human People's Rights: http://wwwl.umn.edu/humanrts/instree/zlafchar.htm

African Charter on the Rights and Welfare of the Child: http://www.childinfo.org/files/fgmc_AfricanCharterontherightsandwelfareofthechild.pdf

American Convention on Human Rights: http://www.oas.org/dil/access_to_information_American_Convention_on_Human_Rights.pdf

American Declaration of the Rights and Duties of Man: http://wwwl.umn.edu/humanrts/oasinstr/zoas2dec.htm

Arab Charter on Human Rights: http://wwwl.umn.edu/humanrts/instree/loas2005.html?msource=UNWDEC19001&tr=y&auid=3337655

Association of Southeast Asian Nations Human Rights Declaration: http://www.asean.org/news/asean-statement-communiques/item/asean-human-rights-declaration

appendix 3 optimum governance structure

COMPONENT	TASKS	RATIONALE
State body or representative that is accountable to the public for the collection, use and access of data held in the registry	I. Identify if there are state bodies that are responsible for registries. 2. Identify if there are state bodies that are responsible for data protection. 3. Identify if there are state bodies that are responsible for medical research oversight. 4. If none in place, identify other bodies that could carry out oversight task.	The state to maintain legitimacy must be able to demonstrate how public data is used. It can have delegated powers to write guidelines when there are new issues that challenge existing legislation.
Management Board that oversees the day to day running of the registry and provides leadership and direction	5. Identify a Management Board who can advise the management team that will provide leadership and be responsible for the registry's activities.	This enables the registry to carry out its tasks efficiently.
Advisory Body that can provide oversight and strategic direction	6. Identify an advisory body that can provide strategic advice to the registry's management team. 7. If no existing body, consider appointing experts and members representative from the general public.	This enables the registry management team to be aware of new developments; how to improve what they already do; how to deal with new challenges.

Access Committee	8. Identify a body that can oversee use, curation and access to the registry and is accountable to the public.	This enables greater accountability as an independent body that gives approval for the use of the registry; but can also provide ethical oversight as required in international law for medical research purposes or access by third parties.
Stakeholder reference groups[96]	9. Identify stakeholders that have an interest in the registry and ensure they are involved for the duration of the program.	These groups will be involved as partners in the development of the registry and its ongoing activities.
Legislation	I0. Identify legislation that applies to registry. II. Establish whether current legislation fit for purpose for the registry. I2. If not, can it be easily amended? I3. Is there other legislation that covers how health information is stored, accessed and shared across geographical and health-sector boundaries?	Legislation applies to all and is enforceable in the courts. It provides a framework for registry activities but may not answer all of the issues that the registry faces.
Guidance	I4. If there is no legislation in place, identify if there is guidance that applies that could be used for a registry I5. New guidance may have to be written to codify existing practice or to develop new practice.	Guidance may have appropriate authority if it is issued by a body that is respected and trusted by all stakeholders.

Policy	I6. The registry may write policy specifically for the registry to cover the procedures that need to put in place to codify the collection, storage and transfer of data.	This makes those using and accessing the registry clear about their responsibilities and duties in regard to the data held in the registry.
Public Engagement	I7.The registry may keep the public informed about the registry by maintaining a website of current activities, appointing public representatives to the various registry committees; providing information on how data is used for public benefit; getting support from government, politicians and key stakeholders.	The registry depends upon public support and trust to maintain its activities.
Compliance Measures	I8. The registry must develop ways to ensure that there are not unauthorised uses of the data without appropriate sanctions.	This helps to ensure the ethical use of the data and helps to promote public trust.

references

I. Bhutta ZA, Black RE. Global Maternal, Newborn, and Child Health — So Near and Yet So Far. New England Journal of Medicine 2013; 369(23): 2226-35.

2. Filippi V, Ronsmans C, Campbell OM, et al. Maternal health in poor countries: the broader context and a call for action. Lancet 2006; 368(9546): 1535-41.

3. Ronsmans C, Graham WJ. Maternal mortality: who, when, where, and why. The Lancet 2006; 368(9542): 1189-200.

4. Graham WJ, Ahmed S, Stanton C, Abou-Zahr C, Campbell OM. Measuring maternal mortality: an overview of opportunities and options for developing countries. BMC medicine 2008; 6: 12.

5. Campbell OM, Graham WJ. Strategies for reducing maternal mortality: getting on with what works. Lancet 2006; 368(9543): 1284-99.

6. Commission on Information and Accountability in Maternal and Child Health. Keeping Promises, Measuring Results. Geneva: World Health Organization, 2011.

7. Independent Expert Advisory Group. A World that Counts: Mobilising the data revolution for sustainable development. In: Group IEA, editor.: United Nations 2014.

8. Chan M KM, Lob-Levyt J, Obaid T, Schweizer J, Sidibe, M, et al. . Meeting the Demand for Results and Accountability: A Call for Action on Health Data from Eight Global Health Agencies. PLoS Med 2010; 7(1).

9. Kim JY. Data for better health—and to help end poverty. The Lancet 2012; 380(9859): 2055.

10. Press release: Better use of data will transform the healthcare landscape, says expert report: European Commission, May 7, 2012.

11. Gates M. Bridging the Gender Gap: How big data can improve the lives of a billion women and girls. Foreign Policy. 2013 July 17, 2013.

12. Gates M. Measure for Measure: We can make dramatic progress in lowering maternal mortality -- but we need better data, and more of it. Foreign Policy. 2013 January 31, 2013.

13. Lee LM, Thacker SB. The cornerstone of public health practice: public health surveillance, 1961--2011. Morbidity and mortality weekly report Surveillance summaries (Washington, DC : 2002) 2011; 60 Suppl 4: 15-21.

14. Choi BCK. The Past, Present, and Future of Public Health Surveillance. Scientifica 2012; 2012: 26.

15. Declich S, Carter AO. Public health surveillance: historical origins, methods and evaluation. Bulletin of the World Health Organization 1994; 72(2): 285-304.

16. Drolet BC, Johnson KB. Categorizing the world of registries. Journal of biomedical informatics 2008; 41(6): 1009-20.

17. Solomon DJ, Henry RC, Hogan JG, Van Amburg GH, Taylor J. Evaluation and implementation of public health registries. Public health reports (Washington, DC : 1974) 1991; 106(2): 142-50.

18. van der Veer SN dKN, Ravelli AC, Tenkink S, Jager KJ. Improving quality of care. A systematic review on how medical registries provide information feedback to health care providers. International journal of medical informatics 2010; 79(5): 305-23.

19. Gissler M. Registration of births and induced abortions in the Nordic countries. Finnish Yearbook of Population Research 2010; 45: 171-8.

20. Gissler M, Louhiala P, Hemminki E. Nordic Medical Birth Registers in epidemiological research. European journal of epidemiology 1997; 13(2): 169-75.

21. Langhoff-Roos J, Krebs L, Klungsoyr K, et al. The Nordic medical birth registers - a potential goldmine for clinical research. Acta Obstet Gynecol Scand 2013.

22. Irgens LM. The Medical Birth Registry of Norway. Epidemiological research and surveillance throughout 30 years. Acta Obstet Gynecol Scand 2000; 79(6): 435-9.

23. Furu K, Wettermark B, Andersen M, Martikainen JE, Almarsdottir AB, Sorensen HT. The Nordic countries as a cohort for pharmacoepidemiological research. Basic & clinical pharmacology & toxicology 2010; 106(2): 86-94.

24. Labrique AB, Pereira S, Christian P, Murthy N, Bartlett L, Mehl G. Pregnancy registration systems can enhance health systems, increase accountability and reduce mortality. Reproductive health matters 2012; 20(39): 113-7.

25. Goudar SS, Carlo WA, McClure EM, et al. The Maternal and Newborn Health Registry Study of the Global Network for Women's and Children's Health Research. International journal of gynaecology and obstetrics: the official organ of the International Federation of Gynaecology and Obstetrics 2012; 118(3): 190-3.

26. Kendall T, Langer A. Critical maternal health knowledge gaps in low- and middle-income countries for the post-2015 era. Reprod Health 2015; 12: 55.

27. Dreyer N, Garner S. Registries for robust evidence. JAMA : the journal of the American Medical Association 2009; 302(7): 790-1.

28. Molina-Ortiz EI, Vega AC, Calman NS. Patient registries in primary care: essential elements for quality improvement. The Mount Sinai Journal of Medicine 2012; 79: 475-80.

29. Williamson OD, Cameron PA, McNeil JJ. Medical registry governance and patient privacy. Medical Journal of Australia 2004; 181(3): 2.

30. The Partnership for Maternal Newborn and Child Health. Essential Interventions, Commodities and Guidelines for Reproductive, Maternal, Newborn and Child Health. Geneva, Switzerland, 2011.

31. Lynge E. Implication for epidemiology of disease registers. Public health reviews 1993; 21(3-4): 263-70.

32. Lawlor DA, Stone T. Public health and data protection: an inevitable collision or potential for a meeting of minds? International Journal of Epidemiology 2001; 30(6): 1221-5.

33. Ingelfinger JR, Drazen JM. Registry research and medical privacy. The New England journal of medicine 2004; 350(14): 1452-3.

34. Hansson M. Where should we draw the line between quality of care and other ethical concerns related to medical registries and biobanks? Theoretical medicine and bioethics 2012; 33(4): 313-23.

35. Hansson MG, Simonsson B, Feltelius N, Forsberg JS, Hasford J. Medical registries represent vital patient interests and should not be dismantled by stricter regulation. Cancer epidemiology 2012; 36(6): 575-8.

36. Wartenberg D, Thompson WD. Privacy Versus Public Health: The Impact of Current Confidentiality Rules. American journal of public health 2010; 100(3): 407-12.

37. Rubel A. Justifying Public Health Surveillance: Basic Interests, Unreasonable Exercise, and Privacy. Kennedy Institute of Ethics Journal 2012; 22(1): 1-33.

38. Tovi MD, Muthama, Mutua Nicholas. Addressing the challenges of data protection in developing countries. European Journal of Computer Science and Information Technology 2013; 1(2): 1-9.

39. Policy Engagement Network. Electronic health privacy and security in developing countries and humanitarian operations. London: London School of Economics and Political Science, 2010.

40. World Health Organization and International Telecommunication Union. eHealth and Innovation in Women's and Children's Health: a baseline review based on the findings of the 2013 survey of CoIA countries. In: WHO and ITU, editor. Geneva; 2014.

41. Luna D, Otero C, Marcelo A. Health Informatics in Developing Countries: Systematic Review of Reviews. Contribution of the IMIA Working Group Health Informatics for Development. Yearbook of medical informatics 2013; 8(1): 28-33.

42. Thomson Reuters Foundation. Patient Privacy in a mobile world: A framework to address privacy law issues in mobile health. London, 2013.

43. Hofferkamp J. Standards for Cancer Registries Volume III: Standards for Completeness, Quality, Analysis, Management, Security and Confidentiality of Data. Springfield, IL: North American Association of Central Cancer Registries, 2008.

44. Ponemon Institute Research Report. 2014 Cost of Data Breach Study: Global Analysis, 2014.

45. http://www.idtheftcenter.org/ITRC-Surveys-Studies/2014databreaches.html. 2014.

46. Ogilvy M, Kollias J. Operating principles for running a clinical quality registry: are they feasible? ANZ journal of surgery 2012; 82(11): 832-7.

47. Sheen A, Katta V, Costello B, Longjohn M, Mantinan K. Registry-based BMI Surveillance: A Guide to System Preparation, Design, and Implementation: Altarum Institute, 2011.

48. Jefferson A, Lambe S, Chaisson C, Palmisano J, Horvath K, Karlawish J. Clinical research participation among aging adults enrolled in an Alzheimer's Disease center research registry. J Alzheimers Dis 2011; 23(3): 443 - 52.

49. McAfee T, Grossman R, Dacey S, McClure J. Capturing tobacco status using an automated billing system: steps toward a tobacco registry. Nicotine & tobacco research : official journal of the Society for Research on Nicotine and Tobacco 2002; 4 Suppl l: S3l-7.

50. Parkin DM. The evolution of the population-based cancer registry. Nature reviews Cancer 2006; 6(8): 603-l2.Gynaecology and Obstetrics 20l2; ll8(3): l90-3.

5l. Phipps E, Harris D, Brown N, et al. Investigation of ethnic differences in willingness to enroll in a rehabilitation research registry. Am J Phys Med Rehabil 2004; 83(l2): 875 - 83.

52. Subhani S, Al-Rubeaan K. Design and development of a web-based Saudi National Diabetes Registry. Journal of diabetes science and technology 20l0; 4(6): l574-82.

53. Korngut L, MacKean G, Casselman L, et al. Perspectives on neurological patient registries: a literature review and focus group study. BMC Medical Research Methodology 20l3; l3(l): l35.

54. McEvoy P, Laxade S. Patient registries: a central component of the chronic care model. Br J Community Nurs 2008; l3(3): l27 - 8.

55. Gliklich R, Dreyer N, Leavy M (eds.). Registries for Evaluating Patient Outcomes: A User's Guide (3rd edition). Rockville, MD: Agency for Healthcare Research and Quality; 20l4.

56. Lopez A, Thomason J. Civil registration and vital statistics? Everybody's business but nobody's business. The Lancet 20l3; 38l(9874): l275-6.

57. Knudsen LB, Olsen J. The Danish Medical Birth Registry. Danish medical bulletin l998; 45(3): 320-3.

58. Axelsson O. The Swedish medical birth register. Acta Obstet Gynecol Scand 2003; 82(6): 49l-2.

59. Oomman N, Mehl G, Berg M, Silverman R. Modernising vital registration systems: why now? The Lancet 20l3; 38l(9875): l336-7.

60. Barrett G, Cassell J, Peacock J, Coleman M. NCR: National survey of British public's views on use of identifiable medical data by the National Cancer Registry. BMJ (Clinical research ed) 2006; 332(7549): l068 - 72.

6l. Muir CS, Demaret E. Cancer registration: legal aspects and confidentiality. In: Jensen OM, Parkin, D.M., MacLennan, R., Muir, C.S., Skeet, R., ed. Cancer Registration: Principles and Methods. Lyon: Oxford University Press; l99l.

62. O'Brien KS, Soliman AS, Awuah B, et al. Establishing effective registration systems in resource-limited settings: Cancer registration in Kumasi, Ghana. Journal of registry management 2013; 40(2): 70-7.

63. von Tigerstrom B, Ries NM. Cancer surveillance in Canada: analysis of legal and policy frameworks and tools for reform. Health law journal 2009; 17: 1-49.

64. European Network on Cancer Registries. Guidelines on Confidentiality and ethics for population-based cancer registration and linked activities in Europe, 2011.

65. Schroll H, Christensen RD, Thomsen JL, Andersen M, Friborg S, Sondergaard J. The Danish model for improvement of diabetes care in general practice: impact of automated collection and feedback of patient data. International journal of family medicine 2012; 2012: 208123.

66. Bygrave L. Data Privacy Law: An International Perspective. Oxford: Oxford University Press; 2014.

67. Greenleaf G. Sheherezade and the 101 data privacy laws: Origins, significance and global trajectories. Journa of Law, Information, and Science 2013.

68. Hickey GL, Grant SW, Cosgriff R, et al. Clinical registries: governance, management, analysis and applications. European journal of cardio-thoracic surgery : official journal of the European Association for Cardio-thoracic Surgery 2013; 44(4): 605-14.

69. Stillman FA, Kaufman MR, Kibria N, Eser S, Spires M, Pustu Y. Cancer registries in four provinces in Turkey: a case study. Globalization and health 2012; 8: 34.

70. North American Association Central Cancer Registries. Procedure Guidelines for Cancer Registries. Springfield, IL: National Cancer Institute, 2001.

71. Black J. Critical reflections on regulation. Australian Journal of Legal Philosophy 2002; 27: 1-35.

72. Kaye J. From single biobanks to international networks: developing e-governance. Human Genetics 2011: 1-6.

73. Laurie G. Reflexive governance in biobanking: on the value of policy led approaches and the need to recognise the limits of law. Human Genetics 2011; 130(3): 347-56.

74. Lopez A, Mikkelsen L, Rampatige R, et al. Strengthening civil registration and vital statistics for births, deaths and causes of death: resource kit. Luxemberg: World Health Organization, 2013.

75. European Commission. Biobanks for Europe - A Challenge for Governance. Luxembourg: Publications Office of the European Union; 2012.

76. Chilton A. Recent Developments in Health Law: Brazil's Pregnancy Registration Requirement and International Commitments to the Rights of Women. Journal of Law, Medicine, and Ethics 2012; 40: 696.School of Economics and Political Science, 2010.

77. Informed Consent for Patient Registries: Draft White Paper for Third Edition of "Registries for Evaluating Patient Outcomes: A User's Guide". Registries for Evaluating Patient Outcomes: A User's Guide. Rockville, Maryland: Agency for Healthcare Research and Quality; 2011.

78. Illman J. Cancer Registries: Should Informed Consent Be Required? Journal of the National Cancer Institute 2002; 94(17): 1269-70.

79. Baird W, Jackson R, Ford H, et al. Holding personal information in a disease-specific register: the perspectives of people with multiple sclerosis and professionals on consent and access. J Med Ethics 2009; 35(2): 92 - 6.

80. O'Doherty KC, Burgess MM, Edwards K, et al. From consent to institutions: designing adaptive governance for genomic biobanks. Social science & medicine (1982) 2011; 73(3): 367-74.

81. Willison DJ, Schwartz L, Abelson J, et al. Alternatives to project-specific consent for access to personal information for health research: what is the opinion of the Canadian public? Journal of the American Medical Informatics Association : JAMIA 2007; 14(6): 706-12.

82. Barrows RC, Clayton PD. Privacy, Confidentiality, and Electronic Medical Records. Journal of the American Medical Informatics Association 1996; 3(2): 139-48.

83. Rindfleisch TC. Privacy, information technology, and health care. Commun ACM 1997; 40(8): 92-100.

84. Hodge J, Gostin, LO, Jacobsen, PD. Legal issues concerning electronic health information: privacy, quality, and liability. Journal of the American Medical Association 1999; 282(15): 1466-71.

85. Broome CV, Horton HH, Tress D, Lucido SJ, Koo D. Statutory basis for public health reporting beyond specific diseases. Journal of urban health : bulletin of the New York Academy of Medicine 2003; 80(2 Suppl 1): i14-22.

86. Hosein G. Privacy and Developing Countries. Canada: Office of the Privacy Commissioner of Canada, 2011.

87. Avancha S, Baxi, A, Kotz, D. Privacy in Mobile Technology for Personal Healthcare. ACM Computing Surveys 2012; 45(1): 3-54.

88. Hosein G, Nyst C. Aiding Surveillance: An exploration of how development and humanitarian aid initiatives are enabling surveillance in developing countries. Social Science Electronic Publishing; 2013.

89. World Health Organization. Legal frameworks for eHealth: based on the findings of the second global survey on eHealth. Geneva: World Health Organization, 2012.

90. Martinez-Perez B, de l Torre-Diez, I, Lopez-Coronado, M. Privacy and Security in Mobile Health Apps: A Review and Recommendations Journal of Medical Systems 2015; 39(181).

91. Africa: Data protection heats up. 2014. http://www.dataguidance.com/dataguidance_privacy_this_week.asp?id=2188 (accessed May 18, 2014.

92. Meingast M, Roosta T, Sastry S. Security and Privacy Issues with Health Care Information Technology. Engineering in Medicine and Biology Society, 2006 EMBS '06 28th Annual International Conference of the IEEE; 2006 Aug. 30 2006-Sept. 3 2006; 2006. p. 5453-8.

93. Hussein H. Dialing Down Risks: Mobile privacy and information security in global development projects. Washington, DC: New America Foundation, 2013.

94. Fernández-Alemán JL, Señor IC, Lozoya PÁO, Toval A. Security and privacy in electronic health records: A systematic literature review. Journal of biomedical informatics 2013; 46(3): 541-62.

95. Pencarrick Hertzman C, Meagher N, McGrail KM. Privacy by Design at Population Data BC: A case study describing the technical, administrative, and physical controls for privacy-sensitive secondary use of personal information for research in the public interest. Journal of the American Medical Informatics Association : JAMIA 2013; 20(1): 25-8.

96. National eHealth Strategy Toolkit. Geneva, Switzerland: World Health Organization and the International Telecommunication Union, 2012.