Principled Health Information Systems:

Ethics Beyond Data Security

December 2019

Principled Health Information Systems

Ethics Beyond Data Security

December 2019

James C. Thomas, MPH, PhD, MEASURE Evaluation
Andreas Reis, MD, MSc, World Health Organization
Victoria Fleming, MA, MEASURE Evaluation

MEASURE Evaluation
University of North Carolina at Chapel Hill
123 West Franklin Street, Suite 330
Chapel Hill, NC 27516 USA
Phone: +1 919-445-9350
measure@unc.edu
www.measureevaluation.org

This publication was produced with the support of the United States Agency for International Development (USAID) under the terms of MEASURE Evaluation cooperative agreement AID-OAA-L-14-00004. MEASURE Evaluation is implemented by the Carolina Population Center, University of North Carolina at Chapel Hill in partnership with ICF International; John Snow, Inc.; Management Sciences for Health; Palladium; and Tulane University. Views expressed are not necessarily those of USAID or the United States government. TR-19-360
ISBN: 978-1-64232-169-2

ACKNOWLEDGMENTS

We are grateful to the United States Agency for International Development (USAID) for its support for this publication, which aims to help countries design digital data systems with an eye to public health ethics, and the importance of protecting the privacy and confidentiality of the individuals who seek services from or interact with the health system.

The authors thank Eugene Kirzhner for his early assistance in identifying relevant documents.

We also thank the knowledge management team of MEASURE Evaluation at the University of North Carolina at Chapel Hill, for editorial, design, and production services.

AUTHOR BIOGRAPHIES

James C. Thomas is an associate professor of epidemiology and director of the MEASURE Evaluation project in the Carolina Population Center at the University of North Carolina in Chapel Hill (UNC). MEASURE Evaluation is USAID's flagship project for strengthening health information systems (HIS) in low- and middle-income countries. Dr. Thomas is also active in public health ethics. He was the principal author of the American Public Health Association's Code of Ethics and served as an ethics advisor to the Director of the U.S. Centers for Disease Control and Prevention. In the context of HIS strengthening, Dr. Thomas addresses ethics in HIS.

Andreas Reis is the co-lead of the Global Health Ethics Team in the Department of Information, Evidence and Research at the World Health Organization (WHO) in Geneva, Switzerland. His work focuses on public health ethics, in particular on ethical issues arising during infectious disease outbreaks, as well as on ethics of public health surveillance. Dr. Reis has lectured and organized trainings for WHO in more than 40 countries and is serving on the editorial boards of *Public Health Ethics* and *Monash Bioethics Review*. He has published widely and is the co-editor of three books on bioethics and public health ethics.

Victoria Fleming is an executive assistant for the MEASURE Evaluation project at UNC. She earned a Master of Arts in History from Appalachian State University, NC.

Suggested citation: Thomas, J.C., Reis, A., & Fleming, V., (2019). Principled Health Information Systems: Ethics Beyond Data Security. Chapel Hill, NC, USA: MEASURE Evaluation, University of North Carolina.

CONTENTS

FIGURE

TABLE

ABSTRACT

Low- and middle-income countries are in the process of creating and expanding digital data systems to monitor their health trends and guide their health programs. The construction of these systems is often regarded as a purely technical task, with little consideration given to its ethical dimensions. One notable exception is attention to data security. To identify a broader range of ethical concerns, we carried out a scoping review of the literature for sets of principles to guide the development and use of digital information systems relevant to population health. The 11 sets we identified named a total of 34 principles, of which data security was one. We organized the principles into four stages of health information system (HIS) development: HIS design, data collection, data storage, and data use. To accommodate these principles, countries must first be aware of them and identify the staff responsible for addressing them in the design of their digital data systems.

Keywords: ethics; health information systems; developing countries

ABBREVIATIONS

AHIMA	American Health Information Management Association
CDC	United States Centers for Disease Control and Prevention
COPASAH	Community of Practitioners on Accountability and Social Action in Health
EMR	electronic medical record
HIS	health information system
LMIC	low- and middle-income country
MOH	ministry of health
UN	United Nations
USAID	United States Agency for International Development
WHO	World Health Organization

INTRODUCTION

In recognition of the many factors needed to improve health through health care in low- and middle-income countries (LMICs), development agencies increasingly pursue health care strengthening in terms of whole systems (De Savigny 2009; U.S. Agency for International Development [USAID] 2014). Healthcare delivery systems are, in turn, informed by systems of health data collection and use, known as health information systems (HIS). By one definition, HIS "integrate data collection, processing, reporting, and use of the information necessary for improving health service effectiveness and efficiency through better management at all levels of health services" (Sauerborn and Lippeveld 2000). Components of an HIS typically include civil registration and vital statistics, disease surveillance, electronic medical records (EMRs), supply chain records, surveys, and program evaluations. Recently, health data and HIS have been recognized as cornerstones for reaching the health-related Sustainable Development Goals (United Nations [UN] 2015; World Health Organization [WHO] 2016).

Many LMICs are currently converting part or all of their HIS into a digital format. The change is driven in part by growing country economies, falling prices for computer hardware, increased expectations for real-time data, global processes from which countries do not want to be excluded, and global expectations that, if not met, may put at risk their receipt of donor assistance. Although access to healthcare is embedded in the Universal Declaration of Human Rights (UN 1948), and health itself is named as a fundamental right in the World Health Organization (WHO) constitution (WHO 2006), the creation and maintenance of the information system that informs healthcare provision are often seen as purely technical tasks without consideration to their ethical dimensions.

Yet, HIS and their management have serious ethical implications that need to be adequately addressed in policies and governance mechanisms. The potential harm to individuals, and thus the ethical implications of an HIS, is perhaps seen most clearly and frequently in the hacking of EMR databases. The U.S. Department of Health and Human Services reported that in 2016, healthcare data breaches, each affecting 500 or more people, occurred on average nearly five times a week (U.S. Department of Health and Human Services 2016). By one estimate, EHRs are 10 times more valuable than credit cards on the black market (Experian 2016). In the case of identity theft, a health record provides more information, including a social security number, residential addresses, and information on children and jobs.

Data security is perhaps the most commonly recognized ethical dimension of an HIS, but it is not the only one. Additional concerns are included in lists produced by professional societies and organizations. For example, the American Public Health Code of Ethics lists 12 principles (Thomas et al. 2002). Among them are providing an opportunity for people affected by a public health policy to have input into its creation and implementation; and ensuring that health services are provided equitably. HIS are a vital part of public health. With the potential to harm and benefit the populations they serve, ethical implications permeate HIS.

Principles are foundational by definition. (We use the term "principle" broadly, to include ethical values, concepts, and prescribed practices.) Thus, any principles guiding the intentions of a system should be identified before the system is created. HIS in many LMICs are currently in the creation phase, and thus there is an opportunity to guide the establishment of HIS with suitable ethical principles. We performed a scoping review of sets of principles put forward by organizations or agencies that manage or use digital information systems relevant to health. It was not our aim to elaborate on, or evaluate, each principle, although we do note a few principles that were not mentioned by any organization or agency. Nor is our purpose to promote any of the sets of principles. Rather, we seek to expand the range of issues that HIS stakeholders recognize as ethical.

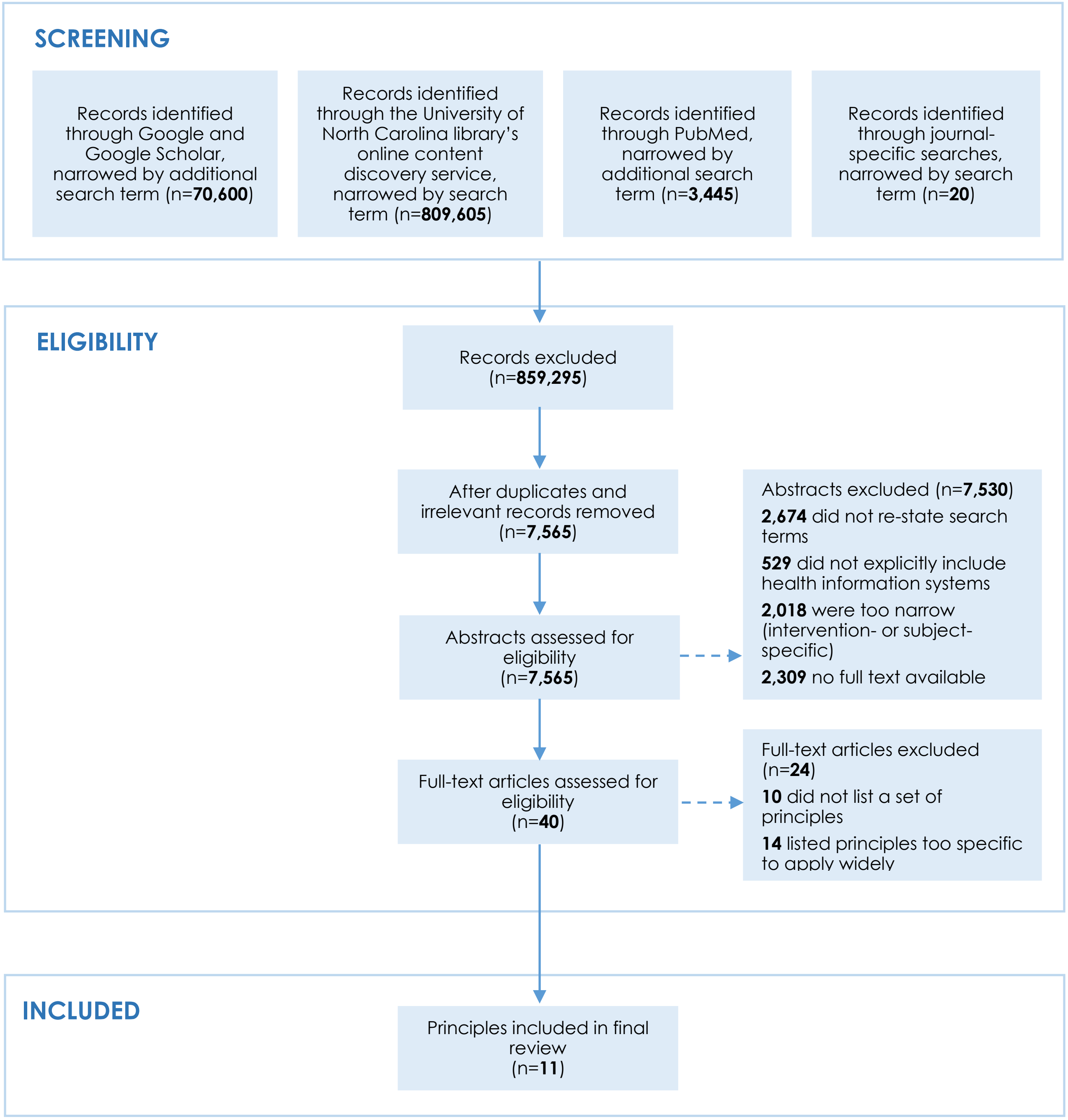
METHODS

We conducted searches from 2007 through 2087 for reports, books, peer-reviewed articles, and other publications containing a set of principles relevant to the development and maintenance of digital health information systems. We did not search for sets of principles that apply to digital data in general, such as the European Union's General Data Protection Regulation (GDPR). We used several digital search tools: Google search engine, Google Scholar, PubMed, and the University of North Carolina library's online content discovery service (which searches across hundreds of thousands of online databases). Our initial search terms were "principles for digital public health," "principles for ethics health systems," "responsible data approach principles," "responsible data approaches public health," and "public health principles." We narrowed the searches further by adding "ethics" if it was not already in the initial search phase, or "big data," "low income," "middle income," or "analytics." In addition, we reviewed the contents of 14 peer-reviewed journals known to publish articles relevant to HIS and ethics for the years 2007 to 2017. They were: American Journal of Public Health; American Journal of Bioethics; Bioethics; Developing World Bioethics; Hastings Center; Ethics and Information Technology Journal; Information Technology and Management Journal; International Journal of Public Health Management and Ethics; Hastings Center Reports; Journal of Health Policy, Politics and Law; Journal of Law, Medicine, and Ethics; Journal of Medicine and Philosophy; Public Health Ethics; and Science and Engineering Ethics.

From our work on HIS, there were a few relevant publications we knew about in advance. They served as sentinel indicators of whether a given search was capturing relevant documents. When the addition of a new term to narrow a search resulted in the loss of a known relevant article, we refrained from adding the additional search term. This initial identification resulted, however, in several over-lengthy lists of publications. Nonetheless, we visually searched the titles in these lists for articles that might be relevant (see Figure 1). After removing irrelevant records, and duplicates, from consideration we were left with roughly 7,500 results to review by abstract or summary were applicable.

This scoping method resulted in a list of 35 articles and documents with relevant sets of principles. From the references of these documents, we identified five more. For the final selection, we included only those sets that addressed information systems broadly, as opposed to focusing solely on a narrower system component, such as data security.

Figure 1. Literature search and identification procedure



RESULTS

The Sets of Principles

We identified 11 documents with a relevant set of principles (American Health Information Management Association 2014; Aranow 2013; Australian Institute of Health and Welfare 2006; International Medical Informatics Association 2016; Kanaan and Carr 2009; Oxfam 2015; Lee and Gostin 2009; Kloss 2016; UN General Assembly 2014; UN Global Pulse 2016; Waugaman 2016). Some of the principles were stated in more traditionally recognized ethical terms, such as rights, while others derived from such principles but were written as the practical implementation of the principle. Some sets used both ethical and practical language. For example, the American Health Information Management Association grouped about 40 practices under eight principles: accountability, transparency, integrity, protection, compliance, availability, retention, and disposition. Oxfam grouped 21 practices under five rights: the right to be counted and heard, the right to dignity and respect, the right to make an informed decision, the right to privacy, and the right to not be put at risk. In tabulating the principles (Table 1), we focused primarily on the practical implementation of broader ethical principles.

Each set was developed by a particular group for a distinct purpose, and each of them highlighted principles relevant to their particular concern, resulting in variation among the sets. Eight of the 11 documents explicitly addressed health information; three address broader information systems in which health is often a component. In this latter category, the discussion paper Principles for Digital Development, a paper that was generated by deep dive discussions that involved a community of 100 organizations led by the USAID Global Development Lab, are intended to be relevant to technology-enabled development programs, including but not limited to HIS (Waugaman 2016) In this instance, the term "digital development," perhaps unintentionally, carries two meanings: the development of the digital technology, and technologies intended to facilitate the development of communities and LMICs. The UN's Fundamental Principles of Official Statistics is another set not limited to health (UN General Assembly 2014). They mention economic, demographic, social, and environmental purposes. We considered healthcare as a type of social service.

The health-related sets varied still further in their purposes. For example, the Australian Health Ministry was addressing principles for health data on indigenous minorities (Australian Institute of Health and Welfare 2006). The American Health Information Management Association was addressing the governance of clinical and operational information to improve the quality of patient care, increase efficiency and effectiveness, and reduce costs and risks (American Health Information Management Association 2014). Writing from the perspective of the U.S. Centers for Disease Control and Prevention (CDC), Lee and Gostin's goal was to propose a strategy for protecting public health data that are exempt from the Health Insurance Portability and Accountability Act (HIPAA) (U.S. Department of Health and Human Services 2003). Because each set was highlighting a particular purpose, the absence of a principle mentioned in another set should not be construed as non-endorsement or non-recognition of the principle.

Patterns among the Sets

We tallied the principles mentioned explicitly or implicitly in each set, showing which lists held principles in common and which had unique principles (Table 1). Because each document described the principles in its own language, it was unclear in some instances whether the respective authors wholly shared each other's meanings. For example, two sets identified the principle of limiting population data collection and use to legitimate government purposes. Lee and Gostin used the term "legitimate public health purposes," while the UN resolution on Fundamental Principles of Official Statistics stated that official statistics need to "meet the test of practical utility" in informing the government about "the economic, demographic, social and environmental situation" (Lee and Gostin 2009; UN General Assembly 2014). Whether the intent of these two sets of authors is the same is open to interpretation.

Some commonly used terms, such as confidentiality, privacy, and security, have overlapping meanings. For example, data are kept secure in part to protect patient confidentiality. One can infer this overlap where confidentiality is a named principle, but security is not, and vice versa. However, some lists mention both.

While admonishing the reader to keep such differences in mind, we summarize here the ethical principles mentioned across the sets. For convenience, we grouped the principles into four stages of HIS development and use: (1) design, (2) data collection, (3) data storage, and (4) data use. However, in many instances, these categories are not mutually exclusive.

(1) HIS Design

The HIS design is the system blueprint. It specifies not only the types of data to be collected and how they are to be transferred to the place of analysis, but the values inherent to the system. For example, does the HIS intend to make summarized data available to the public? Will the software construction be an open, "wiki" process, or one conducted and maintained by a single entity? Values such as these are necessarily identified before the system is built because they determine essential elements of data collection, storage, and use. The specifications are then incorporated into computer code and system policies.

Transparency was the most frequently mentioned principle of information system design. Transparency entails making known the system policies, standards, and procedures. Following best practices was the second most frequently listed. The practices in question varied, including, for example, accepted scientific methods. Although not explicitly stated, scientific practices would include care for representativeness in sampling, procedures to ensure data quality, and giving a prominent role to trustworthy data in decision making. Similarly, some documents noted the importance of using best practices as they relate to digital system design, policies, and procedures. According to some sets of principles, one of those practices would be the creation and use of a data governance committee to oversee the creation of system policies and practices. That could include a means of ensuring that the data are collected and used for legitimate purposes and determining how to evaluate whether the system is adhering to its policies and achieving its intended purposes.

A few of the sets identified efficiency as a principle, with particular attention to the careful use of scarce funding and the time of those who collect and use the data. One means of efficiently using resources, or avoiding redundant efforts, is effective coordination and collaboration. Two of the sets noted that one form of coordination is including the eventual data users in the design of the system. Doing so might help identify data that are not needed, for example, or provide lessons learned from the users' involvement in other information systems.

In a few instances, the concerns of the communities reflected in the data were mentioned. A community could be affected, for example, if it was a minority in the population and was described with data in ways that further marginalized it. The two principles mentioned in only one set were both in the USAID Global

Development lab led Principles for Digital Development: create for sustainability and build for scale (Waugaman 2016). The interest in sustainability stems from the fact that digital information systems in LMICs are typically developed and implemented by experts from developed countries. It is a current best practice in international development to not create dependencies on other countries. Thus, in this case, "sustainability" implies that the host country can maintain the system itself once it is completed and running. Building for scale can be regarded as an element of sustainability. It stands in contrast to a proliferation of systems with narrow purposes or small population reach, which would be harder to sustain than a single system that benefits the whole population.

Table 1. Principles mentioned directly or indirectly in each source addressing the development of information systems relevant to population health. The principles under each of the four headings are listed in order of their frequency mentioned.

	AIHW 2006	Kanaan and Carr 2009	Lee and Gostin 2009	Aranow 2013	Kloss 2013	AHIMA 2014	UNGA 2014	Oxfam 2015	IMIA 2016	Waugaman 2016	UN Global Pulse 2016
HIS Design											
Transparent processes	●	●			●	●	●	●	●		
Follow best practices	●	●			●	●	●			●	
Data governance committee, policies			●	●	●	●					
For legitimate purposes, appropriate uses			●				●		●		●
Enable system evaluation, accountability		●			●	●				●	
Build for efficiency of effort and cost					●		●			●	
Collaborate and coordinate	●						●			●	
Observe community rights	●		●								●
Include HIS users in the design	●									●	
Create for sustainability										●	
Build for scale										●	
Data Collection											
Collect minimum data necessary	●	●	●		●		●	●	●		●
Ensure data quality		●	●	●	●	●		●			●
Comply with the local laws	●		●			●	●	●			●
Obtain consent when appropriate	●	●						●	●		●
Stricter standards in vulnerable populations	●		●					●		●	●
Ensure data timeliness		●		●		●	●				

	AIHW 2006	Kanaan and Carr 2009	Lee and Gostin 2009	Aranow 2013	Kloss 2013	AHIMA 2014	UNGA 2014	Oxfam 2015	IMIA 2016	Waugaman 2016	UN Global Pulse 2016
Provide privacy in data collection			●					●			
Freedom to withdraw from data activity								●			
The right to be counted								●			
Data Storage											
Maintain data security	●	●	●	●	●	●	●	●	●	●	●
Maintain confidentiality, privacy	●	●	●		●	●		●		●	●
Employ a data steward		●		●		●			●		
Data status and uses knowable by subjects		●							●		
Policies for retention and disposal						●					
Data Use											
Control access to the data	●	●	●	●	●	●		●	●		
Use minimum necessary information	●	●	●			●		●	●		●
Provide access to the source community	●	●		●	●	●		●	●		
Disseminate to relevant stakeholders	●	●	●			●	●				
Data sharing agreements		●	●			●					●
To improve health services and the HIS	●			●						●	
Sensitivity to cultural differences	●							●		●	
Educate to enable data use, interpretation	●	●		●							
Opportunity for dissent on interpretation							●				

(2) Data Collection

Once designed, funded, equipped, and staffed, the system begins data collection. As alluded to in the design phase, discussed above, many (8) of the sets of principles noted the need to avoid overburdening data collectors with requests for information that is not essential to guiding health programs. Often, data are collected by those with other duties, such as providing clinical services. The HIS must strike a balance between using data to inform those services and interfering with the delivery of services because of data collection demands.

Two of the principles mentioned pertain to data relevance in terms of its quality or reliability, and timeliness. Inaccurate data can result in misguided policies, which in turn can result in misappropriation of resources or practices that are counterproductive. Data that are reliable but available only months later are not helpful for immediate decision making.

Six of the principles addressed the rights of the people whose data are collected. First, data should be collected legally. When appropriate, as when the data are personal and sensitive, the person about whom information is being collected should be informed of how the data will be used, and their consent should be obtained for it to be used that way. Data collectors should practice higher standards with vulnerable populations, such as assurances against consequences when interviewing prisoners. Two sets of principles then noted that those data should be collected in a manner that provides privacy when the responses are given. Oxfam asserted that a respondent should be able to withdraw from a data collection activity (Oxfam 2015). Conversely, they underscored that marginalized populations have a right to be counted and not further marginalized through underrepresentation.

(3) Data Storage

The sets of principles were unanimous in their assertion that data must be held securely. The UN's Fundamental Principles of Office Statistics was the least specific, stating only that statistical agencies need to practice professional ethical standards in data storage. As mentioned above, data confidentiality, privacy, and security are closely related. When addressed separately, it appears that they may be distinguished in terms of the types of information stored (confidentiality) and access to the information (security and privacy). Removal of personal identifiers in some datasets would be an example of protecting confidentiality. Steps to keep the data secure include digital firewalls, minimizing the number of people and offices given access to the data, and providing only the essential data to those who are granted access. The American Health Information Management Association (AHIMA) noted the need for disposal or archiving policies when data are considered of insufficient quality or no longer relevant (American Health Information Management Association 2014). And two organizations asserted that individuals with data in a system have the right to know the status of their data, what it is being used for, and according to one (Kanaan and Carr 2009), to have errors corrected.

A data steward is the person charged with the responsibility of maintaining procedures related to confidentiality and security, as well as other functions, such as keeping data complete and up to date. Several documents included principles related to data stewardship. One document was framed entirely as the principles and practices of health data stewardship (International Medical Informatics Association, 2016).

(4) Data Use

The ultimate goal of designing an HIS, then collecting and storing data, is using it to guide policies and programs. Controlling access to the data for this purpose is a prominent concern among the sets of principles. According to some of them, access must be provided in some form to the source population, and analyses from the data are to be shared with stakeholders. Three sets of principles stipulated that not only should data or analyses be provided to the source population and stakeholders, but those people should be provided with instruction on how to use the data and interpret the findings. The UN Fundamental Principles Population Statistics holds that Offices of Statistics have the right to dissent with others' interpretations of the data (UN General Assembly 2014).

However, access is also to be limited, for example, to ensure that the data are used for legitimate purposes, such as improving health services or the HIS itself. Means of controlling access and guiding data use include data use agreements and providing only the minimum amount of data needed for the stated purposes.

Three sets mentioned cultural sensitivity to marginalized groups. The measures might include data collection that enables comparison between groups (e.g., between males and females, or between minority and majority populations), or presentation in the language of the group so that they can understand what is being said.

DISCUSSION

In the documents identified by our search methodology, we found more than two dozen principles mentioned among the 11 sets. Although all of the organizations and agencies named data security as a principle, they also demonstrated that the range of ethical concerns in HIS extends well beyond data security. Once the security of an HIS has been addressed, those managing it cannot yet consider the ethical concerns to be fully covered. Regardless of the particular purpose, or the set of principles they follow, there will be several more issues with which they will need to be familiar, and other processes and policies they will need to implement to ensure that the HIS is ethically managed.

Our review has a few limitations. Others might interpret the documents reviewed here differently, concluding that some principles we did not see in a set were indeed present, and vice versa. Alternatively, they may prefer different terms or groupings. Furthermore, we focused on sets that addressed national information systems broadly. There are many other documents that go into further detail on particular aspects of an HIS. For example, there are publications available on principles and procedures for data security and for data sharing (American Psychological Association 2015; United States Office of the National Coordinator of Health Information Technology 2015) and for ethics in public health surveillance (WHO 2017). An examination of the documents addressing narrower components or functions of a system might surface additional principles.

We did not examine national laws pertaining to data. Nigeria, for example, has published a guide to Nigerian privacy and data security laws (UN Foundation 2015). Ideally, a nation's laws and regulations embody the society's moral values. However, the creation of laws is a deliberative process that often takes years, whereas digital technologies and possibilities are advancing much more quickly. Advances in ethical thinking often occur in reaction to new digital possibilities. Thus, to stay closer to recent digital developments, we reviewed emerging ethical principles rather than laws.

Our interest was in principles pertaining to data collected explicitly to guide national public health policies and programs. Increasingly, data collected for non-health purposes are being explored for their utility in informing public health. This includes social media and Internet searches, for example. There is a growing literature on principles for using "big data" that were outside the scope of this article (see, for example, Mittelstadt and Floridi 2016; Vayena et al. 2015; Wyber et al. 2015).

The frequency with which particular principles were mentioned in the 11 sets identified is not synonymous with the importance of the principle. As noted above, each of the sets was written with a unique purpose and for a different set of stakeholders. This variety of purposes provides a wider range of perspectives, and presumably a wider range of principles. Because of this range, and because the descriptions of the principles are often open to interpretation, there is no principle that we identify as obviously missing from the comprehensive set. However, virtually all of the principles require more specificity for implementation. Principles such as participation, transparency, and accountability beg the question of who is to participate, what they should be able to see, and to whom the system is accountable. If, as at least one of the sets indicates, the government is to enable the source population to examine the data, for example, then what skills should be taught and what analysis tools provided? The Community of Practitioners on Accountability and Social Action in Health (COPASAH) is one civil society organization whose primary mission is enabling citizens to hold their governments accountable for the quality of health services (www.chsj.org/copasah.html). They might consider developing tools or approaches that focus specifically on community access to and analysis of population health data. Also, the topic-specific documents mentioned above will likely be a source for some of the needed specificity.

With this article, we do not intend to guide in the implementation of the principles. Our goal, rather, has been to bring attention to the ethical dimension of HIS and to describe the range of ethical concerns currently incorporated into the ethics of organizations and agencies concerned with national level systems.

Our hope is that those responsible for designing and implementing a national HIS will recognize the importance of ethical principles in their work and incorporate them into the system governance before experiencing a serious ethical mishap. Integrating ethical policies and procedures into an HIS can foster trust in the systems among the stakeholders, and not least among patients and civil society. Trust, in turn, can result in the provision of more accurate and complete information, and thus a more useful HIS.

Each of the 11 sets identified in our review has a relatively small number of principles. However, complying with any one principle can require several policies and procedures and the resources to equip relevant personnel to implement them. When the full range across all 11 is considered, the number of policies and procedures could be daunting. Furthermore, because wrestling with an institution's principles is less concrete than writing a computer code, there will be a temptation to focus time and resources on the more concrete tasks, while neglecting the less concrete ones.

To make ethics more concrete, a country might start with the identification of the staff responsible for attending to the ethical dimension of the HIS and assessing the degree to which they are equipped for the task (Spigel and Wambugu 2018). Those charged with addressing the ethical dimension of an HIS may need some training in practical ethics. Establishing the authority and resources to implement policies and procedures will also be essential.

Individuals and offices in this role will find it helpful to interact with similar bodies in other countries. This might be achieved, in part, through the creation of an online HIS ethics resource center or a community of practice. All HIS governance bodies will benefit from documents providing guidance on international standards for procedures and institutional structures. Each of these steps requires resources for personnel, training, and computer hardware and software. Several of these steps should also be informed by research into the best practices. Many countries will require support in scaling up their HIS systems, both financially as well as conceptually. But, at present, there is little evidence that bilateral and multilateral donors and foundations are giving attention to ethics beyond data security. Our hope is that the range of ethical issues described here will incite them to address a wider range of issues.

REFERENCES

American Health Information Management Association. (2014). Information governance principles for healthcare. http://www.ahima.org/~/media/AHIMA/Files/HIM-Trends/IG_Principles.ashx.

American Psychological Association. (2015). Data sharing: Principles and considerations for policy development. http://www.apa.org/science/leadership/bsa/data-sharing-report.aspx.

Aranow, M. (2013). The seven practices of health care data governance. The Advisory Board Company, IT Strategy Council. https://www.advisory.com/-/media/Advisory-com/Research/ITSC/Research-Notes/2013/The-Seven-Simple-Practices-of-Health-Care-Data-Governance.pdf.

Australian Institute of Health and Welfare. (2006). National aboriginal and Torres Strait islander health data principles. http://www.health.gov.au/internet/main/publishing.nsf/content/B92E980680486C3BCA257BF0001BAF01/$File/health-plan.pdf.

De Savigny, D., & Adam, T. (Eds.). (2009). Systems thinking for health systems strengthening. Alliance for Health Policy and Systems Research. Geneva: Alliance for Health Policy and Systems Research, WHO. http://apps.who.int/iris/bitstream/10665/44204/1/9789241563895_eng.pdf.

Experian. (2016). Third annual 2016 data breach industry forecast. Experian data breach resolution. http://www.experian.com/assets/data-breach/white-papers/2016-experian-data-breach-industry-forecast.pdf.

International Medical Informatics Association. (2016). The IMIA code of ethics for health information professionals. http://imia-medinfo.org/wp/wp-content/uploads/2015/07/IMIA-Code-of-Ethics-2016.pdf.

Kanaan, S. B., & Carr, J. M. (2009). Health data stewardship: What, why, who, how. National Committee on Vital and Health Statistics. https://www.ncvhs.hhs.gov/wp-content/uploads/2014/05/090930lt.pdf.

Kloss L. Precyse HIM Innovation Community. (2016). Health information management in 2016: Guiding principles and a governance framework for a digital age. http://www.quovadimuscomm.com/wp-content/uploads/2014/03/HIM-2016-white-paper-final.pdf.

Lee, L. M., & Gostin, L. O. (2009). Ethical collection, storage, and use of public health data: A proposal for a national privacy protection. JAMA, 302(1), 82–84.

Mittelstadt, B., & Floridi, L. (2016). The ethics of big data: Current and foreseeable issues in biomedical contexts. Sci Eng Ethics, 22, 303–341. https://www.ncbi.nlm.nih.gov/pubmed/26002496.

Oxfam. (2015) Responsible Program Data Policy. https://oxfamilibrary.openrepository.com/bitstream/handle/10546/575950/ml-oxfam-responsible-program-data-policy-en-270815.pdf;jsessionid=564A13E4AFEB92A2D3495E801B2A138F?sequence=1.

Sauerborn, R., & Lippeveld, T. (2000). Introduction. In T. Lippeveld, R. Sauerborn, & C. Bodart (Eds.), Design and implementation of health information system. World Health Organization. http://apps.who.int/iris/handle/10665/42289.

Spigel, L., Wambugu S., Villella, C. (2018). MHealth Data Security, Privacy, and Confidentiality Guidelines: Companion Checklist. MEASURE Evaluation, University of North Carolina at Chapel Hill. https://www.measureevaluation.org/resources/publications/ms-17-125b/at_download/document

Thomas, J. C., Sage, M., Dillenberg, J., & Guillory, V. J. (2002). A code of ethics for public health. Am J Public Health, 92(7), 1057–1059.

United Nations (UN). (1948). The universal declaration of human rights. United Nations General Assembly Resolution 217 A. http://www.un.org/en/universal-declaration-human-rights/.

United Nations (UN). (2015). Sustainable Development Goals. http://www.un.org/sustainabledevelopment/sustainable-development-goals/.

United Nations (UN) Foundation. (2015). Keeping personal health information safe and secure: A guide to privacy and data security laws in Nigeria. http://www.unfoundation.org/assets/pdf/keeping-personal-health.PDF.

United Nations (UN) General Assembly. (2014). Fundamental principles of official statistics. Resolution 68/261. Adopted by the General Assembly on January 29, 2014. https://unstats.un.org/unsd/dnss/gp/FP-New-E.pdf.

United Nations (UN) Global Pulse. (2016). Privacy and data protection principles. https://www.unglobalpulse.org/privacy-and-data-protection-principles.

United States Office of the National Coordinator of Health Information Technology. (2015). Guide to privacy and security of electronic health information, version 2.0. https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf.

U.S. Department of Health and Human Services. Breach portal: Notice to the secretary of HHS breach of unsecured protected health information. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

U.S. Agency for International Development (USAID). (2014). Local systems: A framework for supporting sustained development. https://www.usaid.gov/sites/default/files/documents/1870/LocalSystemsFramework.pdf.

Vayena, E., Salathé, M., Madoff, L. C., & Brownstein, J. S. (2015). Ethical challenges of big data in public health. PLoS Comput Biol, 11(2), 1–7.

Waugaman, A. (2016). Principles to practice: Implementing the principles for digital development. Washington, DC: The Principles for Digital Development Working Group. http://www.unicefstories.org/wp-content/uploads/2013/08/From_Principle_to_Practice.pdf.

World Health Organization (WHO). (2006). Constitution of the World Health Organization. 45th Edition, Supplement. http://www.who.int/governance/eb/who_constitution_en.pdf.

World Health Organization (WHO). (2016). Global diffusion of eHealth: Making universal health coverage achievable. http://who.int/goe/publications/global_diffusion/en/.

World Health Organization (WHO). (2017). WHO guidelines on ethical issues in public health surveillance. http://apps.who.int/iris/bitstream/handle/10665/255721/9789241512657-eng.pdf;jsessionid=6C55E024DB6A20CC6E47075DC4CEA3A8?sequence=1.

Wyber, R., Vaillancourt, S., Perry, W., Mannava, P., Folaranmi, T., & Celi, L. A. (2015). Big data in global health: Improving health in low- and middle-income countries. Bull World Heal Organ, 93(3), 203–208.

MEASURE Evaluation
University of North Carolina at Chapel Hill
123 West Franklin Street, Suite 330
Chapel Hill, North Carolina 27516 USA
Phone: +1-919-445-9350
measure@unc.edu
www.measureevaluation.org

This publication was produced with the support of the United States Agency for International Development (USAID) under the terms of MEASURE Evaluation cooperative agreement AID-OAA-L-14-00004. MEASURE Evaluation is implemented by the Carolina Population Center, University of North Carolina at Chapel Hill in partnership with ICF International; John Snow, Inc.; Management Sciences for Health; Palladium; and Tulane University. Views expressed are not necessarily those of USAID or the United States government. TR-19-360
ISBN: 978-1-64232-169-2