Electronic Health Privacy and Security in Developing Countries and Humanitarian Operations

A report prepared by the Policy Engagement Network

PEN paper 7

Electronic Health Privacy and Security in Developing Countries and Humanitarian Operations

A report prepared by the Policy Engagement Network for the International Development Research Centre

December 2010

THE LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE

Table of contents

Executive Summary 3

About this Study 4

Methodology 4

Introduction 6

Medical Privacy in Principle 8

Medical Privacy in Practice 14

Organisational Dynamics of Data Practices 16

Capturing the Users and Understanding Empowerment 16

Analysing eHealth Systems 20

Privacy, Security, and Design Implications 21

Policy Implications 23

Opportunities for Securing Medical Privacy and Health Information 26

Implementing Partners 26

International community 26

Funders 27

Next steps 27

Concluding remarks 27

Annex 28

Executive Summary

- Expertise on the privacy and security aspects of the eHealth systems being deployed in resource-constrained environments such as developing countries and humanitarian operations is severely lacking; the knowledge base in this space is similarly weak;

- To be effective, the principles and aspirations for medical privacy enshrined in international agreements, policies, and commitments must be supported by a local awareness of privacy responsibilities, a strong national legal and regulatory footing, and the appropriate use of information and communication technology;

- Among the legal and regulatory requirements for strong privacy and security protections are respect for self-determination, the appropriate and proportionate collection, management, access and disclosure of medical information, and strong mechanisms for monitoring compliance and accountability;

- Within developing country and humanitarian operation contexts, there is a wide and diverse range of social, ethical and gender considerations related to medical privacy which must be more fully appreciated by those involved in developing eHealth systems; the user must not be taken for granted;

- Threat models must also consider the organisational risks to medical privacy and health information security in these resource-constrained environments, such as insider threats and intra-organizational data-sharing;

- Any 'solutions' to medical privacy or health information security in these contexts will need to incorporate both technological means such as directed identifiers, access controls and encryption, as well as appropriate organisational, legal and policy responses;

- Any decision by funders, designers, or implementers to exclude these privacy and security mechanisms from an eHealth system must be made as the result of informed deliberation rather than as a matter of expediency.

About this Study

Although we have extensive experience in privacy and security of information systems, as both academics and practitioners, our work in developing countries and humanitarian operations is relatively recent.

In 2008 we began work with the United Nations High Commissioner for Refugees to review their registration systems and to analyse data collection risks. Alongside our partnering organisation, Privacy International, we also began to work with the International Development Research Centre (IDRC) to conduct research on privacy challenges in developing countries. We quickly realised that our work in these domains would be drastically different to anything we had previously encountered. Our traditional recommendations would be meaningless. Calling for policy change, for instance, is insufficient in environments with minimalist legal frameworks, or where the rules are easily suspended as in the case of emergency humanitarian and relief efforts. Similarly, the rate of deployment of technologies in these environments was unlike anything we had ever encountered. Yet we also saw how the status of 'vulnerable' can be assigned to an entire population and even an entire region. We encountered real risks that we had considered previously only in the abstract.

In 2009 we began discussions with international organisations regarding privacy and security frameworks. In particular, in June 2009 IDRC invited us to engage with their partners on health projects in Asia. The conversations that followed were enlightening as we were able to learn about innovative techniques and practices being deployed in developing countries that had not yet even been deployed elsewhere. Based on our earlier experiences in developing countries and humanitarian operations, we grew concerned about informational privacy and security. We approached IDRC to ask if we could assist the organisation and its partners in considering the matter further.

Methodology

Our research approach is based on the methodology of *engagement*. Recognising that much of the wisdom in a domain already exists within, we begin by consulting experts and practitioners to advise on relevant literature and empirical studies, and to hear their own experiences so that we are grounded in their

contexts. IDRC was a key partner in helping to identify these individuals and organisations. We also made extensive use of our own existing networks, through interviewing and consulting with leading academics, technology developers, policy and legal professionals, medical practitioners, and development experts. Throughout this process we moved back and forth between conducting consultations with experts in the field and expanding our reviews of the literature to increase our competence and our ability to engage further.

We quickly encountered the key research challenge for this domain: while there are many experts and resources on medical informatics and privacy, too few consider developing countries and humanitarian operations. Worryingly, the converse also appears true: while there are many experts and resources on medical informatics in developing countries, too few study and understand privacy.

These gaps were illuminated by the workshops we organised and attended.

- expertise on the technological and ethical dimensions of medical informatics were well understood amongst the participants in our London workshop, but few had worked in developing countries;
- security and privacy frailties within the design of the technologies were well understood amongst participants of the technology workshop in Washington, DC, yet the legal frameworks were mostly ignored, and users were assumed to be empowered and knowledgeable;
- our workshops and consultations around the OpenMRS and MedInfo conferences in Cape Town were full of insight on local modalities in many countries, including the interests in protecting confidentiality, but legal frameworks were often identified as weak, while developers were sometimes focused on delivering functioning solutions rather than considering ethical and quasi-legal concepts that were considered *foreign*.

We consulted with some of the largest software and hardware developers, both in the traditional medical informatics space (e.g. General Electric, Phillips) and the new and emerging companies who are building the platforms of the future (e.g. Google, Microsoft, Nokia). We delivered our initial findings at an academic workshop at the University of Oxford, and sought more guidance at the International Conference of Data Protection and Privacy Commissioners in Jerusalem.[1] We quickly realised that many people were encountering the same challenges, and that there was no incumbent body of knowledge or literature.

Rather than trying to be that incumbent, we hope that this study will instead provide food for thought so as to inspire greater resources to enter this domain. Dangerous decisions occur too often where the risks are so high and where awareness is so low. As we are building new infrastructures in countries that we all hope to exist for decades to come, getting this right *now* requires a great collection of minds and resources. It is indeed possible we may not get a second try.

[1] See the Annex for details on these engagement activities.

Introduction

Privacy is challenging. It is both ancient and modern. It challenges the status quo and it also frustrates change. It is progressive and regressive. Yet in the provision of healthcare it is essential. Ensuring that information is processed lawfully and fairly, and is kept secure, is a common value of everyone involved in healthcare.

In every country with strong legal traditions and safeguards, privacy is already mandated even though the risks may be low. In every advanced technological society and context, privacy is near the top of policy and technological agendas, with varying levels of success.

In developing countries and humanitarian relief operations, where people are most vulnerable, worryingly there is little consideration of privacy policy and technology. In fact, where poor privacy practices may make already vulnerable people even more vulnerable, privacy is often perceived as an impediment to their care. Where it matters most is where it is mostly ignored.

In developing countries and humanitarian operations, information on patients is often essential. Public health surveillance relies on collection and sharing protocols. Multiple points of access and care providers must be able to gain access to information about patients in order to ensure continuity of care. Researchers require this information to study these situations and to improve processes, and save lives.

Now that *eHealth* is high on the agendas of governments, the international community (including funding agencies), industry, and civil society, the application of new technologies will disrupt this unstable ecosystem even more so. The deployment of technologies as diverse as mobile devices and national data processing centres will result in the collection and processing of even greater amounts of information. The ongoing drive to increase the interoperability of once discrete health systems further complicated the dynamcis of healthcare provision. Yet this need not conflict with privacy. Privacy and eHealth may even complement one another.

The purpose of this study is to identify the current dynamics regarding eHealth privacy and security in developing countries and humanitarian operations. In this report, we understand eHealth to cover a wide range of information and communication

technologies, from electronic medical records to systems for managing and tracking patients, test results, medications, diseases and so forth. Through extensive discussions with practitioners, developers, industry, health specialists, regulators, civil society and academics we have developed an understanding of the risks and value of new forms of managing medical information.

As a result, this report is therefore not trying to preach on why privacy is important, nor to debate its value. This report has three audiences.

1. IDRC: As an active organisation in this field, it enables and partners with those who are deploying eHealth solutions. More than that, IDRC prides itself on its applied research focus. It must therefore be aware of the privacy and security concerns emerging from the introduction of information and communication technologies to improve health outcomes and health equity.

Being a Canadian Crown Corporation, it also reflects Canadian traditions and values, with its respect for rights and freedoms. In fact Canada has one of the most advanced legal regimes for the protection of privacy, with a multi-layered regulatory framework, all of which has been reflected in Canada's own work on medical informatics.[2]

In turn, we recommend methods and mechanisms by which IDRC can ensure that the best available techniques are considered in its work abroad.

2. The international development community: As the enablers of much of the technological change in eHealth, members of this community must be made aware of the risks of failing to attend to privacy and security. After all, why should the international community fund the development of a system in an African or Asian country with weaker safeguards and more fallible procedures than a system installed in an American or European hospital? Of course values and resources may differ, but the exclusion of safeguards and procedures must be done deliberately rather than through expediency.

3. Practitioners and developers: While practitioners and developers may represent a variety of communities, they are working closely to develop new systems and practices that manage personal information under the rubric of *eHealth*. In our discussions with general practitioners their awareness of privacy and confidentiality was quite high, but the awareness of technological options to protect privacy was low.

Meanwhile our discussions with developers had mixed results: while some understood information security and medical confidentiality quite well, the majority did not, and sometimes perceived it as a hindrance. The two communities now have a shared set of challenges in privacy and security that they must consider within the variety of conditions in developing countries and humanitarian and relief operations. Just as security and privacy cannot be ignored, we equally cannot transplant security and privacy techniques from abroad that may not be adaptable, particularly as legal frameworks may be lacking.

Beyond these targeted audiences, we expect other actors in the public health and eHealth communities to benefit from the report's findings. These other players might find certain aspects of the report enlightening or instructive, but for whatever reason (e.g., they are outside the report's sphere of influence) are not expected to alter their behaviours or actions.

---

[2] Cf. 'Electronic Health Records and the Personal Information Protection and Electronic Documents Act', a report funded by the Office of the Privacy Commissioner of Canada, by the University of Alberta Health Law Institute and the University of Victoria School of Information Science, April 2005.

Medical Privacy in Principle

The processing of information is part and parcel of the provision of healthcare. At the most simple level, patients have information that they share with medical staff, and medical staff impart information unto patients. At the most complex, we see a myriad of institutions sharing and generating information on the patients and medical staff in order to manage the provision of healthcare.

Information must flow for the entire system to function. Each individual and institution must share information. Compulsion to share information becomes ethically challenging, however, and this is why the relationship between the patient and the doctor has long been regulated on the basis of trust. The original Hippocratic oath included the duty of the care-giver to 'keep secret' and 'never reveal' 'all that may come to my knowledge'. The modern version of the oath is more explicit on 'privacy', "I will respect the privacy of my patients, for their problems are not disclosed to me that the world may know." The concern is that if there are no promises of confidentiality, then the patient will not disclose information, and worse, may forego treatment.[3] There is evidence that individuals may not even seek testing if their confidentiality is not assured.[4]

This principle has been enshrined in the practice of medicine, and in turn, in international statements, policies, and commitments. Several examples are provided below:

- **The World Health Organization** places an emphasis on health and human rights, wherein privacy is crucial, particularly as it is enshrined in international human rights covenants. These covenants aim to protect the dignity and autonomy of the individual through minimising and restricting interferences.
- **The World Medical Association Declaration of Helsinki on the Ethical Principles for Medical Research Involving Human Subjects**[5] states

[3] This was the principle applied by the U.S. Supreme Court in *Jaffee v. Redmond*, in 1996, protecting the relationship between a patient and a psychotherapist: "Effective psychotherapy depends upon an atmosphere of confidence and trust, and therefore the mere possibility of disclosure of confidential communications may impede development of the relationship necessary for successful treatment. The privilege also serves the public interest, since the mental health of the Nation's citizenry, no less than its physical health, is a public good of transcendent importance."

[4] 'Concerns over confidentiality may deter adolescents from consulting their doctors: A qualitative exploration', J Carlisle, D Shickle, M Cork, A McDonagh, Journal of Medical Ethics, 32, 133-137, 2006; and 'HIV test-seeking before and after the restriction of anonymous testing in North Carolina', I Hertz-Picciotto, L Lee, C Hoyo, American Journal of Public Health, 86, 1446-1450, 1996.

[5] Adopted in June 1964, with amendments in 1975, 1983, 1989, 1996, and 200; available at http://www.who.int/bulletin/archives/79%284%29373.pdf

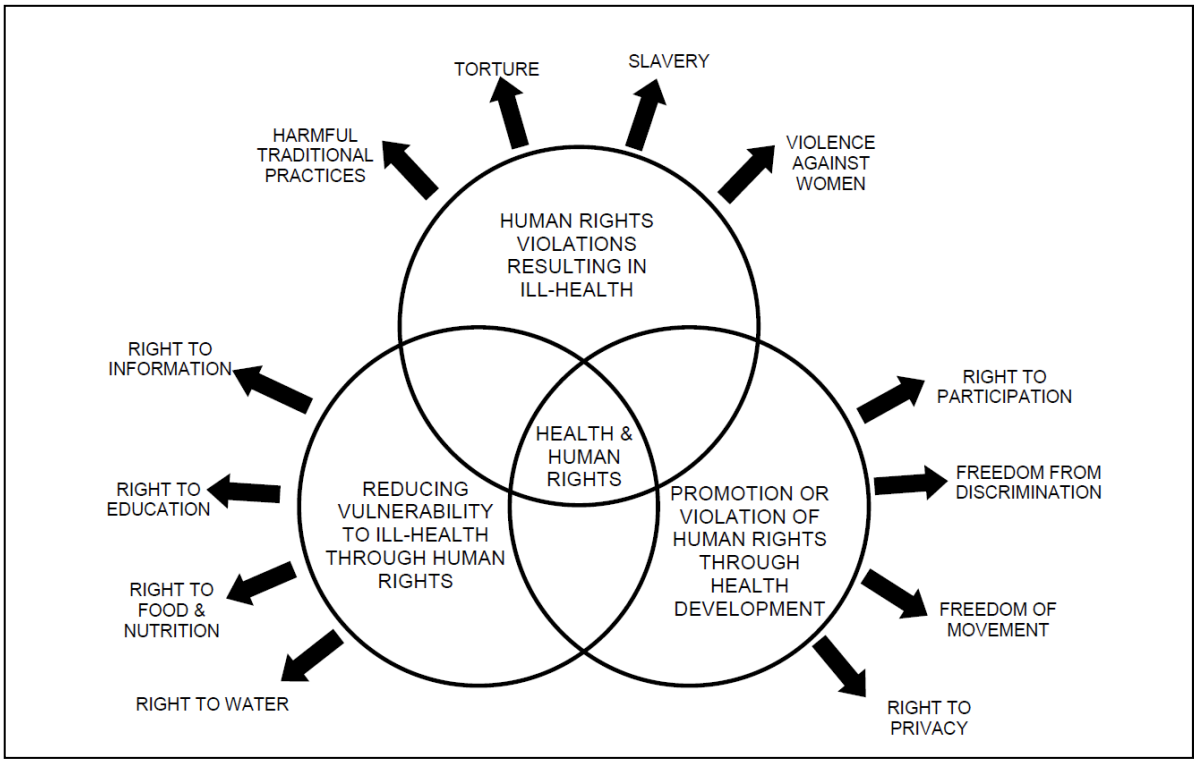
that "every precaution should be taken to respect the privacy of the subject, the confidentiality of the patient's information and to minimize the impact of the study on the subject's physical and mental integrity and on the personality of the subject". Furthermore it outlines the nature of consent that is required from research subjects.

- **UNAIDS** also considers human rights as a crucial component of its work: using health information for public health goals must be balanced against individuals' rights to privacy and confidentiality. Individuals must be protected against mandatory testing; HIV status must be kept confidential.[6] Laws must be developed in countries to protect these rights. Importantly, funding organisations are called on to comply with the guidelines and make funding available to implement them – in fact 'maintaining security and confidentiality must be a condition for funding.'[7]

International organisations also have their own confidentiality guidelines to which their staff must adhere. For example, the International Committee of the Red Cross (ICRC) has long argued that any information it collects must be kept confidential in order for it to do its job, and failing to protect data could place individuals at risk.[8] Strong safeguards against disclosure are sometimes necessary; for instance, warring parties are likely to restrict access of the ICRC if they believe that the organisation may be collecting information for future use, e.g. in a criminal proceeding.[9]

But these are merely initial steps in a complex area. These 'rights' and 'principles' only have strength when they are supported by local

Figure 1 - From the World Health Organisation '25 Questions and Answers on Health and Human Rights', July 2002.



[6] UNAIDS Political Declaration on HIV, 2006. See http://www.unaids.org/en/AboutUNAIDS/PolicyAndPractice/HumanRights/

[7] UNAIDS Guidelines on Protecting the Confidentiality and Security of HIV Information, Interim Guidelines, Proceedings from the May 2006 Workshop in Geneva, issued May 15, 2007, available at http://data.unaids.org/pub/manual/2007/confidentiality_security_interim_guidelines_15may2007_en.pdf

[8] 'Confidentiality: key to the ICRC's work but not unconditional', Interview with ICRC deputy director of operations, September 20, 2010, available at http://www.icrc.org/eng/resources/documents/interview/confidentiality-interview-010608.htm

[9] 'Recognition of the ICRC's long-standing rule of confidentiality - An important decision by the International Criminal Tribunal for the former Yugoslavia', Stephane Jeannet, ICRC, International Review of the Red Cross, No. 838: 403-425, June 2000.

conditions. To date, these have included the following:

- **Awareness of responsibilities.** Rights are best protected when institutions and individuals are most empowered and aware of these rights. Privacy and security of medical information have been protected best when we are well aware of the risks and accordingly act to ensure that only relevant information is collected, and it is managed with great care. The norms that govern healthcare have, in the past, been strong protectors of privacy and confidentiality.[10]

- **A legal basis.** Rights and principles often require a strong legal footing in order to enumerate and specify rights that grant explicit protections. Many countries around the world have such legal protections in the form of data protection laws with particular emphasis on medical information as 'sensitive' information. Other legal safeguards include constitutional protections, and individuals may use the common law and tort to seek remedies in case of the disclosure of private facts. These ensure that responsibilities are known, accountability is assigned, and remedies are available.

- **Minimal use of technologies.** Perhaps the greatest protector of the privacy and security of medical information to date has been the limited availability of platforms for data-sharing. Information kept on paper in locked cabinets is less likely to be shared en-masse with other institutions. A single healthcare practitioner may keep files under direct supervision, thus limiting the availability of information to other parties. Systems often cannot interact with one another, again limiting the ability of the information to be accessed by third parties, and in turn, used for other (originally unspecified) purposes. This is not a sure-footed safeguard, however, as the paper-based or isolated systems may also limit the possibilities for ensuring confidentiality and security through the use of privacy-enhancing technologies.

In many countries these legal, regulatory, and even normative frameworks interact to provide an environment where medical information is protected. Even in these environments there are concerns about the introduction of technologies to enhance information processing.

Developing countries tend to lack legal and regulatory safeguards. International treaties and conventions may have been signed, but they are not enacted into law. Laws may exist but the regulations that give life to these legal rights may not have been codified, and the ability to gain access to remedies may be limited. What is remarkable is that the norms of confidentiality and privacy may yet exist. In our discussions with practitioners from a number of developing countries we learned that these norms are indeed often practiced, despite the legal and regulatory void.

In our interactions within this domain, we saw that technologies are being introduced that expand data collection and the potential for access and sharing, even though they are not designed to necessarily support the normative safeguards. We are encountering the same level of momentum behind 'eHealth' that we saw with 'e-commerce' and 'e-government'. A key difference is that with these previous initiatives, it was presumed that legal and regulatory frameworks were necessary for adoption. However we are not seeing similar levels of legislative and regulatory activities to support the introduction of eHealth. As a result, any gap between principle and practice will only be exacerbated.

This does not need to be the case. As a healthcare system becomes more complex, the management of information will in turn become more complex. There is a greater need for more elaborate explanations of responsibilities and safeguards, even beyond those enshrined in acts of law. Many medical codes include a more detailed articulation of patients' rights. For instance, the Canadian Medical Association Health Information Privacy Code defines a "patient's right to determine with

[10] One study of American physicians found that there was a strong belief that their ethical and professional obligations, not regulatory mandates, assure patients' privacy and confidentiality. Cf. 'Health Information, The HIPAA Privacy Rule, And Health Care: What Do Physicians Think?', Julia Slutsman et al., Health Affairs, 24(3): 832-842, 2005.

Third party access?
A recent case in the UK illuminates the risks of third party access to certain eHealth systems. In November 2010 it was revealed that users of a website in the UK that provides health advice (known as NHS Choices) have had details of their visit unknowingly communicated to Facebook, Google, and other advertisers and third parties.

The information that is passed on includes details of the ailments or conditions that the user was investigating.

The only way to opt-out of the service is to disable cookies in the web browser, which is impractical as doing so makes navigating the web incredibly difficult. The NHS has been criticized for these data-sharing practices and an investigation is underway.

When a legal framework exists, such tracking and reporting of potentially sensitive and embarrassing information is unacceptable without thorough protections and requiring easy means of establishing and withdrawing consent.

whom he or she will share information and to know of and exercise control over use, disclosure and access concerning any information collected about him or her." Similarly, the British Medical Association has developed a 'tool kit' for confidentiality and disclosure of health information,[11] and the General Medical Council has guidance on the confidentiality of patients' privacy.[12]

These codes are indeed helpful at explaining the responsibilities and duties of the practitioners, yet more thorough legal frameworks are necessary to explain the rights of the patient. The foundation stone of a patient's right in this domain is the treatment of the patient as a human who deserves dignity. This 'dignity' is linked to the human right to life in most constitutional codes, and more explicitly as the constitutional right to privacy, upon which rest all other legal and technological measures.

Legal and regulatory requirements have emerged around the world to elaborate upon the right to privacy in a high-technology environment. Though they vary slightly, the rules from Canada,[13] Europe[14] and the United States (though possibly to a lesser extent[15]), as examples, have a significant level of convergence that include:

Respecting self-determination:

- Requiring informed consent of the individual for the collection, use and disclosure of personal information;
- Providing for a right to withdraw from the system and/or have information deleted;
- Granting the individual a right to access, inspect and copy health information, and to request amendments;

Collection and Management:

- Limiting collection of personal information, limiting use, disclosure and retention;
- Requiring organisations to have established adequate privileges for staff for accessing, reading and writing medical information;
- Duty upon organisations to keep information secure, through administrative safeguards, physical safeguards, and technical safeguards; assisted through risk analysis, policies and

[11] 'Confidentiality and Disclosure of Health Information tool kit', British Medical Association, December 2009. Available at: http://www.bma.org.uk/images/confidentialitytoolkitdec2009_tcm41-193140.pdf

[12] See http://www.gmc-uk.org/guidance/ethical_guidance/confidentiality.asp

[13] 'Electronic Health Records and the Personal Information Protection and Electronic Documents Act', Report prepared with support from the Office of the Privacy Commissioner of Canada, University of Alberta, Health Law Institute and University of Victoria, School of Health Information Science, April 2005.

[14] 'Working Document on the processing of personal data relating to health in electronic health records', Article 29 Data Protection Working Party of the European Commission, adopted February 15, 2007.

[15] 'The HIPAA paradox: The privacy rule that's not', Richard Sobel, Hastings Center Report: 40-51, July-August 2007.

procedures, training, etc., and an explanation to the individual of how information is secured;

Access and Disclosure:

- Developing the ability for individuals to restrict access to their records, possibly in the form of a virtual 'sealed envelope';
- Developing the ability for individuals to discover who has been accessing health information;
- Restricting and regulating secondary uses, and regulating data-sharing, and international transfer;
- Clear restrictions on access by law enforcement and national security agencies, and other non-secondary uses;

Monitoring Compliance and Accountability:

- Notifying individuals of any breach in security and confidentiality;
- Ensuring accuracy of the information;
- Granting individuals the right to review privacy practices, right to challenge compliance and practices, and to seek remedy.

Some of these principles could even aid the provision of health care and the deployment of eHealth solutions. Too rarely do we discuss the integrity and accuracy of medical information held in databases, and a clear governance structure and rights of access by the individual could help to rectify these situations.[16]

These principles may be seen as a starting point, or perhaps as a set of principles upon which practices can be measured. Alternatively they can be seen as context-dependent, and that these principles, though they apply to eHealth, only apply to countries with foundations in human rights, supported by constitutional and legislative safeguards, under the rule of law granting rights to citizens and consumers. Our contention, however controversial, is that if we are to ignore these principles in other environments it should be done with the awareness that we are doing so, and perhaps with some justification as to why these principles may not be applicable.

---

[16] See for instance, 'The woman falsely labelled alcoholic by the NHS', Rob Evans, the Guardian, November 2, 2006, available at http://www.guardian.co.uk/society/2006/nov/02/health.epublic

Abuses and illegal trade in medical information?

Data which are leaked or stolen from insufficiently protected medical databases will inevitably be traded in underground and black markets.

Medical information can be used for profit and intelligence, or to defame and embarrass individuals.

Profit

In Mexico a case arose in which personal data about millions of the country's citizens are being illegally sold by rogue data brokers. These sensitive data originate from various public sector and commercial databases, including records from the federal electoral institute, social security agency, and various banks and credit card companies, among others. These infractions are common, in spite of the fact that Mexico has data protection legislation. Medical databases are not immune to these risks and must be carefully protected in order to prevent additional harm to citizen privacy.

Intelligence

The latest information from documents leaked through the website Wikileaks disclosed that the U.S. State Department was asking its staff to collect information on "political, military, intelligence, opposition, ethnic, religious, and business leaders" in the African Great Lakes region, including their health data, ethnicity, and DNA.

Embarass

In the UK in 2009 the then-Labour Government had devised a plan to allege that the leader of the Opposition party had suffered from an embarrassing medical condition such as a sexually transmitted disease. They had no such medical information but it came at a time when the UK Government was considering a national health record system.

Scrutinise

The Canadian Privacy Commissioner is now investigating how a cabinet minister's briefing notes included the medical and financial information of a critic of the Government's Veterans Affairs, including part of a psychiatrist's report. The individual later discovered that this information had been accessed by hundreds of federal bureaucrats.

These may not always be based on information-intensive practices, nor can they be limited strictly by access controls. In one interview we were told of how a health worker had noticed that a fellow church-goer was sitting in front of the door where treatment occurs for HIV/AIDS patients; and the health worker later notified the local religious leader of her discovery.

Sources:

- **'Tepito vende bases de datos oficiales', El Universal.mx, April 2010 http://www.eluniversal.com.mx/primera/34792.html**
- **'cable 09STATE37561, Reporting and Collection Needs: African Great Lakes (DROC, Burundi, Rwanda), April 2009, available at http://cablegate.wikileaks.org/cable/2009/04/09STATE37561.html**
- **'McBride and Draper emails: 'Gents, a few ideas'', Gaby Hinsliff and Mark Tran, Observer, April 12, 2009.**
- **'Veteran's complaint highlights significant privacy issues', Office of the Privacy Commissioner of Canada, available at http://www.priv.gc.ca/cf-dc/pa/2010-11/pa_20101006_e.cfm**

Medical Privacy in Practice

eHealth systems have much to offer medicine in developing world and humanitarian operations. The deployment of effective technologies to facilitate and manage the provision of healthcare where there was previously little infrastructure will result in leaps and bounds improvement of healthcare. With a weaker legal infrastructure, a likely lack of deliberative and consultative regimes, and scarce resources we will be compelled to question many of the fundamentals of privacy and confidentiality.

Even as countries like the United States and the United Kingdom are trying to deploy electronic medical record systems with varying success, they too are encountering privacy and security concerns.[17] A recent study from the U.S. claims that security and privacy problems result in data breaches that cost the healthcare system billions of dollars, even as it is difficult to detect these breaches in security, and few resources are applied to ensure security and privacy.[18] Meanwhile a recent survey in the U.S. found that 97% of Americans believe that medical institutions should not be allowed to share or sell sensitive health information without consent.[19]

In resource-constrained environments the situation is even more problematic. Neither the patients nor the practitioners are particularly aware of rights and responsibilities.[20] Literacy may be minimal, so notices are insufficient. Populations may be more mobile and therefore patient registration may be even more important and yet difficult to achieve. Care providers may be responsible for larger numbers of patients. Staff may not be trained in procedures. The technical infrastructure may vary, with problems with electricity, so running additional processes and procedures may prove too

[17] 'Do summary care records have the potential to do more harm than good? Yes', Ross Anderson, BMJ 340: c3020, 2010.

[18] 'Benchmark Study on Patient Privacy and Data Security', Ponemon Institute LLC, November 2010.

[19] Zogby International Online Poll conducted for patientprivacyrights, '2000 Adults' views on privacy, access to health information, and health information technology', published November 2010. Findings available at http://patientprivacyrights.org/wp-content/uploads/2010/11/Zogby-Result-Illustrations.pdf

[20] 'The importance of patient privacy during a clinical examination' Shailaja Tetali, Indian Journal of Medical Ethics, IV(2): 65, April-June 2007.

challenging. Multiple organisations may be operating in the same space, with implementing partners and government agencies, whereby it may be difficult to identify the primary custodians of the information. All of these barriers are exacerbated in humanitarian operations.

The greatest irony is that the protection of confidentiality and privacy is perhaps even more important in these very same environments. Different societies have a variety of ideas of what is acceptable, aberrant, and abhorrent. In some countries it is HIV status,[21] in other countries it is your mental health, or whether you are likely to develop diabetes.[22] In our interviews with practitioners in developing countries, they identified a myriad of domains where individuals could be harmed through inappropriate information processing. As examples:

- In many parts of the world women are particularly vulnerable, as they may be discriminated against in the provision of healthcare (if they are even able to seek access to services because of gender discrimination issues, or in the case of mHealth they may not have direct access to mobile devices). This is particularly problematic when involving reproductive rights, including the sensitive issues of sexual activity and abortion.[23]

- The rights of young people, and especially the impoverished and underprivileged, require special attention. Issues of consent become particularly problematic when dealing with these youth in developing country contexts.[24]

- Religion and morals may play stronger roles in social lives, and in turn any information that calls into question an individual's abidance by social and religious morals may hurt that individual's reputation. One's 'moral fibre' may be questioned, thus leading to social exclusion.

- Sexuality is a sensitive topic in nearly all cultures, but the ramifications of wrongful disclosure in some contexts may result in severe actions being taken against individuals, sometimes even involving death.[25]

- Diagnoses can be interpreted in a variety of ways, leading to discrimination, or worse. For instance, the diagnosis of a recessive genetic disorder can also inadvertently reveal non-paternity if the father and child are both tested (a recessive disorder requires the disease causing mutation to be present in both parents and for the child to inherit both copies). There are many countries where adultery is a criminal offence for women and in some cases inadvertent release of such information could lead to severe punishment.

While these are particularly sensitive, they are also integral to many of the health programmes in developing countries. The ailments that lead to stigma and social exclusion are exactly what we need to treat. We need patients to be willing to come forward and share, and not recoil in fear of information being leaked. Once entrusted we need to ensure that our systems and procedures live up the faith they have placed in them.

The most basic safeguard of individual consent is possibly a luxury that is not afforded to individuals in some environments where access may be limited, or even provided through another individual (e.g. in some contexts, women may not access healthcare when it is provided by men, so husbands and fathers will go to the surgeries on

---

[21] 'Religious leaders key in the Middle East's HIV/AIDS fight', Jan McGirk, The Lancet, Volume 372, Issue 9635, 279-280, July 26 2008.

[22] In our discussions and interviews, we heard a number of references to social stigmas, including mental health and diabetes. For referenced examples see 'Experience of social stigma by people with schizophrenia in Hong Kong', by Sing Lee, Margaret T.Y.Lee, Marcus Y.L. Chiu, Arthur Kleinman, British Journal of Psychiatry, 2005 186: 153-157; 'Living on the Edge: The Stigma of Diabetes' MedIndia, November 10, 2008; and 'Social stigma and discrimination: a care crisis for young women with diabetes in India', DiabetesVoice, May 2009, Volume 54, 37-39.

[23] In Indonesia, there are practices of mandatory pregnancy tests, virginity tests, and 'a web of discriminatory laws and practices that deny Indonesian women who become pregnant outside marriage full access to maternal care and reproductive health. 'Left without a choice: Barriers to reproductive health in Indonesia', Amnesty International, 2010. Available at: http://www.amnesty.org/en/news-and-updates/report/indonesia-left-without-choice-barriers-reproductive-health-indonesia-2010-11

[24] 'Obtaining informed consent: observations from community research with refugee and impoverished youth', R. Nakkash et al., J Med Ethics, 35:638-643, 2009.

[25] 'Uganda's Rolling Stone paper told to stop outing gays', BBC News, November 1, 2010.

behalf of the women). If the basic safeguards that are enshrined in rights and principles are too difficult to maintain, then rather than abandoning all safeguards we must seek others, and do so urgently. Otherwise wrongful disclosures can result in the breakdown of family cohesion, social exclusion, and persecution.

Organisational Dynamics of Data Practices

We must also recognize the threats that emerge as a result of the inherent dynamics of health organizations at work – how medical practitioners and administrative staff collect, store, use, and share health information.

It is well established in the field of information security that the greatest threats to an organisation's information assets come from within. The threat of internal abuse of sensitive medical information therefore should not be underestimated when designing threat models and building safeguards for privacy and security. In this context, internal abuse typically involves staff inappropriately accessing or disclosing medical information, without the patient's authorization. These acts are motivated by spite, curiosity, or simply caprice. We learned during our engagement with medical practitioners from the developing world that such incidents regrettably occur all too often and, when sensitive or embarrassing information is disclosed, can lead to patients being chastised by community members.

We must also consider the threat of external abuse of medical information, including unauthorised disclosure through covert channels. Whereas the potential for abuse of medical information stored on paper records is physically limited, abuse is still possible and the consequences great for those affected. Of course the introduction of information and communication technology into the healthcare context multiplies and complicates the risks of outsider abuse of medical information[26], but the fundamental problem is not technological in nature but rather organisational: healthcare organisations are either unable or unwilling to secure their records and guard patient privacy.

External abuse can also result from data-sharing, which too often goes unquestioned by the medical community. In developing countries, data-sharing for medical research or disease surveillance purposes very regularly takes place without patients' awareness or informed consent. A warning of the dangers of these practices and the implications for privacy comes from Haiti: the Haitian government requested the medical records of all individuals infected with HIV from the public health organizations working in the country. Government officials wanted to use the data to populate a national database for calculating and tracking the prevalence of HIV. While many organizations complied, others were hesitant about sharing such sensitive information without first consulting their patients.[27] To our knowledge, Haiti lacks a legal framework for the protection of privacy, and the government does not provide guidance to organisations on how to provide safeguards while information sharing.

Capturing the Users and Understanding Empowerment

In the design of any system we always need to ensure that we capture faithfully the interests and characteristics of the stakeholders. If you wrongly presume that the users are proficient with technology, then you risk building a system that is overly complicated for average users. Likewise, if you wrongly presume that your users are seeking simple solutions, then you are likely to frustrate them with simplistic interfaces and functions. As the user base increases and the scope of use widens, it becomes difficult to envision a single type of user, and so we must design our systems with greater care and with multiple audiences in mind.

The risks are much greater in the design of public-facing systems as there is another stakeholder to consider: the individual. This individual, whose information is being processed by a system can also a citizen or a consumer. In the case of eHealth, the individual patient is sometimes an amalgam of both a citizen and a consumer.

The way we consider these individuals affects the way we design our processes and technologies. In this sense, designing for privacy differs from

[26] 'Privacy, Information Technology, and Health Care', Thomas C. Rindfleisch, CACM, 40(8): 92-100, 1997.

[27] 'Electronic records pose dilemma in developing countries', Nature Medicine, 16(3): 249, March 2010.

Individuals, or Patients, or Citizens?

These abstract notions of human rights are also supported by real data: a recent study in the U.S. found that 93% wanted to be able to decide which government agencies and companies could access their information. Both the U.S. and UK governments have announced recently the ability of individuals to gain access to the information held on them in their medical records.

Figure 2 – from https://www.mymedicare.gov/

When we have raised the rights of patients as citizens and consumers in developing countries and humanitarian operations, we faced resistance from system developers. In these discussions, we were told that individuals in these environments have different concerns, and their priority is gaining access to healthcare. We were told that individuals are not preoccupied with 'western' concepts of individuality. Developers state that they cannot see the importance of asking for consent prior to uploading files and sharing patient information.

For more information please see:

- **Zogby International Online Poll conducted for patientprivacyrights, '2000 Adults' views on privacy, access to health information, and health information technology', published November 2010.**
- **"Blue Button' Provides Access to Downloadable Personal Health Data', the White House, October 7, 2010.**
- **'Patients will control records, says DoH', Kable news, November 10, 2010.**

designing for security, in that only the former considers the essence of the individual and the according responsibilities placed upon the institutions and the technologies. Put simply: citizens and consumers have rights that are not defined or limited by technology. In our experience and in our discussions with many system designers, one of the great challenges in providing care in developing countries and humanitarian operations is that developers make difficult presumptions about the people who are implicated by the systems.

Where there have been policy discussions about the constitution of the 'individual', mostly in North America and Europe, the individual patient is considered a citizen or consumer who can make decisions. As an eHealth policy becomes more developed, the language of individual empowerment emerges almost naturally. This matches well with European human rights laws that require that any eHealth system that collects information must be established either under law or with the consent of the individual. Even if there is a law or consent, the individual still retains his or her rights about how the information is used, and consent may be withdrawn.[28]

We have indeed encountered this first hand in humanitarian operations, where individuals are seeking access to emergency care and services, and are in turn relatively unconcerned with issues around consent or information control. Empowerment comes with access to services that are otherwise inaccessible.

In our discussions with systems developers and policy-makers they applied the same thinking to the security of medical information. In their minds the risks of unapproved information disclosure were quite low: the only users of the systems

[28] Consent Mechanisms for Electronic Health Record Systems: A Simple Yet Unresolved Issue'. K.T. Win and J.A. Fulcher, Journal of Medical Systems, 31, 91-96, 2007.

would be authorised individuals accessing the information for the purpose at hand. The 'western' concerns regarding malicious hackers or security vulnerabilities in software[29] were dismissed because the general population lacked the computing resources to try to break into systems. As a result, security would be sorted out at a later time, if at all. The insider threat was not even considered.

Under the rubric of 'medical informatics for developing countries', many assumptions were being made about the type of environment where these systems may be deployed, and many other assumptions were being made about the types of individuals implicated. It was our impression that the worst case scenario was being considered in both situations: individuals were so much in need of healthcare that they cared for little else; and resources were so poor that the risks of abuse were limited. Put simply, patients are poor and users are noble. Even if this is an adequate assessment of the needs and threats, and from our limited field research and interviews we can say that we were unable to verify such claims, we cannot imagine that this situation necessarily permeates every medical environment in every developing country. Assumptions made in the abstract and enshrined into technology are just another form of universalism.

mHealth and Privacy

Mobile health presents lots of opportunities for healthcare provision, but simultaneously there are new privacy problems emerging:

- **Although mobile phones are arguably *the* success story in the domain of information technology and development, their diffusion still is not universal. Not everyone has a mobile phone. Often phones are shared by families; in some contexts, the head of the household (usually the father) 'owns' the phone (likewise, the dominant male in the household also controls the family's health IDs);**
- **In this scenario, the use of mobile phones for notifying individuals about, for example, a test result, or to remind them to attend an appointment about which their family members were not previously aware is a complicated affair;**
- **What sort of information do you disclose in the text message itself? While it may be possible to exclude specifics about a disease or medication, in certain areas the mere fact that one is being contacted by a health actor can be stigmatizing;**

Therefore, some eHealth systems have started obfuscating these messages, using codes such as sport scores or messages from 'friends' to communicate sensitive health data.

However, there are other complications to the use of mobile phones for health. Across the globe, governments are requiring citizens to register their SIM cards with personal information. An example of this is the case of VidaNet, a HIV patient reminder system in operation in Mexico City, which is currently struggling to provided a privacy-friendly service as the country enforces a national SIM registration program.

Sources:

- **'Mobile phones to improve HIV treatment adherence' Benjamin H. Chi & Jeffrey S. A. Stringer, The Lancet, November 2010. Available at: http://www.thelancet.com/journals/lancet/article/PIIS0140-6736(10)62046-6/fulltext**
- **Cf. 'Mobile Communication and Society: A Global Perspective', Manuel Castells et al., MIT Press, 2009.**
- **'Cell Phone Short Messaging Service (SMS) for HIV/AIDS in South Africa: A literature review', Khatry-Chhetry Mukund Bahadur & Peter J. Murray, Presented at MedInfo, Cape Town, South Africa, 2010.**
- **'Cell-Phone Medicine Brings Care To Patients In Developing Nations', J. Lester Feder, Health Affairs, 29(2): 259-263, 2010.**

[29] See, for example, 'Killed by Code: Software Transparency in Implantable Medical Devices', Karen Sandler et al. Software Freedom Law Center, 2010. Available at: http://www.softwarefreedom.org/resources/2010/transparent-medical-devices.html

To remedy these types of problems, systems designers are compelled to look at more than mere risk perception. Independent risk analyses are needed to complement the consultation with stakeholders. Inadvertent or unintentional breaches and disclosure of personal information are still breaches. We must consider systems and practices that are considered essential in other environments and then must justify why we would exclude such safeguards as we develop systems for developing countries and humanitarian operations. Threat analyses and privacy impact assessments conducted at the earliest of stages assist in identifying and understanding the risks of information collection and processing.

After all, if the development goal is achieved and the societies in which we implement these technologies eventually develop sustainable economies, social structures, and political systems, then it is possible that the same risks that exist in the rest of the world may one day apply in developing countries. The infrastructure that is left behind by our development goals in eHealth may limit that society to choose to move beyond a perceived 'needs'-based approach to one based on the rights of autonomous patients.

Privacy in practice?
In our interviews with systems designers and health workers from developing countries we were excited to discover that a certain kind of privacy innovation is being developed and deployed in various locales.

mHealth systems are incorporating obfuscation and minimal disclosure techniques in order to protect and limit the sensitive information that is transmitted to mobile phone platforms. Sometimes a secret 'friend' sends a coded message to users to remind them about a scheduled check-up; other times it is a sports match update that secretly relays a test result.

These measures further enable the use of mobile technologies for healthcare in a way that is privacy-enhancing.

Analysing eHealth Systems

The specific motivations behind the use of information and communication technologies for healthcare delivery and management in developing countries and humanitarian operations are wide-ranging, and of course depend on the local context and needs. However, in general eHealth technologies are seen as holding the potential to improve health service delivery, expand the delivery of treatment and services, improve patient outcomes, facilitate the 'leap-frogging' of outdated health systems in other countries, and improve disease surveillance, among others.

In order to understand and try to resolve the potential threats to privacy and security introduced by the use of eHealth, we first need to differentiate the different technologies and applications.[30] These include:

1. Electronic health records and electronic medical records that capture and store patient information.[31] These are increasingly being centralized;

2. Laboratory information management systems (often used to report test results to administrators and healthcare staff);

3. Prescription information systems (for ordering, dispensing, and tracking medications) within hospitals, GP offices, and pharmacies;

4. Patient registration and scheduling systems (for tracking and managing the movement of patients);

5. Systems for aggregating and reporting information, monitoring health programs, and tracking patients' status (e.g. district health information systems or health management information systems);

6. Clinical decision support systems;

7. Patient reminder systems (e.g. for prompting patients to take medications or visit a clinic). Within the developing country context, the mobile phone is increasingly being leveraged

[30] See for instance, 'What is eHealth: A Systematic Review of Published Definitions', H Oh, C Rizo, M Enkin, A Jadad, Journal of Medical Internet Research, 7, e1, 2005.

[31] The use of this terminology varies. To some, the 'health record' is the larger statement of the individuals' state of health, sometimes deployed at an organisational, regional or even national scale; while the 'medical record' is often generated by a health organisation or professional.

for these purposes, introducing novel privacy issues;

8. Systems for medical research (used to collect, store, manage, and report data used for research purposes).[32]

Each type of system, depending on the environment and context, involves the processing of different types of personal information, for different purposes. In turn each system will have varying privacy and security risks. A research-based system traditionally has less identity information compared to a patient registration system, but more diagnostic and health information. Labs and pharmacy systems tend to require data-sharing protocols with both local surgeries and national or regional insurance providers. Information becomes the lifeblood of a healthcare system as information is collected, shared, and studied.

Privacy, Security, and Design Implications

From our limited review of eHealth plans in developing countries and humanitarian operations, we see that there is some pull towards bringing all of these systems together under a single authority. If this is the case, eHealth systems may become the largest collection of information on a country's citizenry, and in a way a *de facto* civilian registry.[33] A national registry of citizen information is certainly useful for governments to understand and manage their populations. But these are usually better established for specific purposes through deliberative processes to ensure it is fit for purpose,[34] not built as a side effect of providing healthcare. A population registry could also have many secondary effects that are not well considered while we establish a health registry, as it can for instance reveal ethnic origin or religious affiliation in a systematic manner.

As healthcare provision is not a monolithic exercise of only state actors, the information held within an eHealth infrastructure would be distributed in nature. General practitioners, hospitals, pharmacies, universities, and other institutions would seek to gain access. In some countries we heard of plans for storing all of this information in the 'cloud', where information on a citizenry will be stored in another country, and in turn, another legal jurisdiction. The distributed system and the institutions seeking access may not be governed by the same policies and procedures. If not carefully designed, a single record in one non-state entity could provide the key to gaining access to the entire health record of an individual or even a whole community.

Considering privacy and security at the earliest stages of system design helps to better

---

[32] 'E-Health Technologies Show Promise In Developing Countries'. J. A. Blaya et al., Health Affairs, 29(2): 244-251, 2010.

[33] For a discussion of national identity registries, see 'Global Challenges for Identity Policies' Edgar A. Whitley and Gus Hosein, Palgrave Macmillan, 2009.

[34] See 'Identity Policy: Risks & Rewards: a report prepared for the U.S. Federal Trade Commission', Simon Davies and Gus Hosein, April 2007, available at http://www.ftc.gov/bcp/workshops/proofpositive/ftc-identity-final.pdf

understand the operational environment. For example, no health researcher would ever demand for *carte blanche* access to an EHR database, so the system should be designed as such.[35] Similarly, the managers of a laboratory that has an existing system of registration will not want to re-design their entire system based on a different registration system from a hospital, or even the national system, so persistent and unique identifiers may not be ideal.[36] Equally, granting each user of a given system-component complete access to all information held therein could result in information overload, could be resource-intensive, and if a device is lost or left vulnerable, could result in the loss of important information.[37] It just so happens that these very same decisions are important to privacy and security.

Considering how to implement identifiers, access controls, sharing and disclosure protocols, amongst other system-design decisions is therefore integral to protecting privacy and security. Fortunately there is a growing body of literature within the computer science world on privacy and security of medical informatics, and emerging best practices. These methods include:

- using directed identifiers rather than global identifiers so that a given institution recognises the same patient in different ways, preventing one institution from having the key by which it can access all health information across the system;[38]
- implementing access controls based on roles and privileges so that only some members of staff have access to the relevant personal information, while providing audit trails to make this verifiable;[39]
- considering the use of digital rights management-type systems to secure eHealth records infrastructures, protecting information persistently throughout an enterprise and across organisational boundaries;[40]
- encrypting the databases to ensure that third parties – even those providing cloud services – may not gain access to the information;[41]

---

[35] See the risks of health research and personal information in 'Pan-Canadian De-Identification Guidelines for Personal Health Information', Khaled El Emam et al., a report produced for the Office of the Privacy Commissioner of Canada, April 2007.

[36] For instance, see an interesting discussion regarding the use of Social Security Numbers in the U.S. as patient identifiers: AHIMA e-HIM Work Group on Regional Health Information Organizations (RHIOs). 'Using the SSN as a Patient Identifier.' Journal of AHIMA 77, no.3 (March 2006): 56A-D, available at http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_030976.hcsp?dDocName=bok1_030976

[37] 'The inadvertent disclosure of personal health information through peer-to-peer file sharing programs', Khaled El Emam et al., JAMIA 17:148e158, 2009.

[38] This is an explicit concern of the Canadian Health Infoway Privacy Impact Assessment: "Do safeguards prevent internal identifiers from becoming public (and hence creating new de-facto public identifiers)". 'A 'Conceptual' Privacy Impact Assessment on Canada's Electronic Health Record Solution', Blueprint Version 2, Canada Health Infoway, February 12, 2008.

[39] These must be flexible enough so that workarounds exist for staff to gain access to records to which they have not yet been granted access, e.g. A&E clinicians can be granted greater access by using a shared credential.

[40] 'A Secure Electronic Healthcare Record Infrastructure in the Digital Rights Management Model', Nicholas Paul Sheppard et al., 2009. Available at: http://dspace.ucalgary.ca/bitstream/1880/47561/1/2009-939-18.pdf

[41] 'Deployment of a Highly Secure Clinical Data Repository in an Insecure International Environment', Henry Feldmana et al., presented at MedInfo South Africa 2010.

- ensuring minimal sharing and disclosure through provable means to ensure that only the necessary information is disclosed and shared;[42]
- rendering pseudonymous every single transaction made in a healthcare environment through encryption, where all the institutions that need to know information can access that information, but unauthorised institutions may not;[43]

Because of the massive investment into eHealth and growing concerns about privacy and security, the thinking on these issues will expand significantly in the coming years. eHealth developers and policy-makers must be aware of these developments to ensure that their design choices result in systems that are, in fact, fit for purpose.

It is worth even considering why identifiable information is actually needed in the first place. For instances, in many contexts, such as sexual health clinics, no personal information would be collected at all; or walk-in clinics might ask for name and contact details but patients could provide false identities. There is a drive towards collecting identifiable information, however. Sometimes this is intentional through policy choices, e.g. a government requiring the reporting of HIV cases;[44] or by system design where the individual patient has to be verified against a national registry prior to receiving treatment. At the outset, system designers and policy professionals need to ask why information is necessary before they start deciding which information is to be collected.

Policies also provide an opportunity to deliberate on a technology or technique in a more open manner. For instance, biobanks are spreading around the world[45] yet there is relatively limited debate in developing countries about this practice of linking biological tissues to an individual's medical record. As they expand, these collections will raise additional issues due to the dual-use of DNA as a biometric identifier -- giving rise to governments' interest in gaining access to such data for policing purposes -- and as an indicator of familial relationships. A policy framework and a policy discussion will help to ensure that techniques like these are deployed as is strictly necessary for the desired purpose.

Policy Implications

Technologies are not the only solutions as thorough procedures are also required to make sure these protections are enforceable. For instance, role-based access control is not a perfect stand-alone system. These access control systems are often designed in such a way that if there is an emergency and medical practitioners need to access medical information that is encrypted or otherwise secured, then they may 'break the glass' and gain emergency access. While this sounds reasonable, the glass is very often broken: one study in Norway found that 54% of 99,352 patient records were accessed through such means; over a single month 295,000 'emergency' cases were logged, and the practice was widespread amongst staff where over 40% of the over 12,000 authenticated users had 'broken the glass'.[46]

---

[42] One health information systems project in Malawi encountered such issues with their use of two-dimensional bar code stickers on the Malawi 'health passport'. To facilitate the quick processing of patients at the clinic, these stickers were affixed on the cover of passports. However, the project provided HIV/AIDS patients with specially coloured stickers, and so their status was unintentionally disclosed whenever patients would reveal their passports. A simple yet elegant solution to this problem was putting the stickers inside the passport, thereby reducing the risk of unintentional disclosure.

[43] 'An anonymous healthcare system', Melissa Chase & Kristin Lauter, Microsoft Research, presented to the USENIX 2010 Workshop on Health Privacy and Security, August 2010.

[44] e.g. 'New State Law on HIV and AIDS Names Reporting', available at http://www.cchealth.org/services/hiv_aids/hiv_names_reporting_2006_05.php

[45] See for instance 'Global Directory of Biobanks, Tissue Banks, and Biorepositories', available at http://www.specimencentral.com/biobank-directory.aspx

[46] 'Access Control and Integration of Health Care Systems: An Experience Report and Future Challenges.' L. Rostad et al., Presented at the Second International Conference on Availability, Reliability and Security in Vienna: 871-878, 2007. Available at: http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=4159886

The policy landscape?
We must consider the variety of laws and policies within a given jurisdiction, and abroad, as we deal with eHealth. The existence of constitutional and statutory provisions regarding privacy are certainly a start, including the protection of privileged communications between a patient and a health professional; the existence of codes of practices; and data protection laws. It is also important to consider the other policies that may interact with the eHealth systems.

As examples:
- **SIM registration laws may affect the adoption of mobile telephony in a country. If individuals are unable to prove their identity because of a lack of documentation, for instance, they would be prevented from having a mobile device.**
- **Data retention laws and practices may necessitate the collection and retention of information about users communications and transactions. This could mean that both patients' and health professionals' communications could be subject to surveillance, and this information could be kept for extended periods of time.**
- **The existence of a national register or a national identity system could inter-operate with an eHealth system; but equally it could damage the provision of health services to those who remain undocumented.**

Just as procurement laws may affect the choice of technologies, these policies may introduce new challenges for eHealth.

Policies are therefore necessary to ensure against abuse, to provide safeguards, and to ensure adequate remedies. As mentioned above, national legislation on patient privacy and comprehensive data privacy laws are key first steps. Individuals' rights are then made clear, as is the legal basis for any eHealth system, and the qualification of consent.[47] Legislation will help to ensure that every institution is aware of the responsibilities to keep information private and secure. Importantly, legislation can also require that privacy is built into the system through the required use of the 'privacy impact assessments', 'privacy by design' principles, and 'privacy-enhancing technologies' that are growing more popular around the world.

At a more local level, each organisation also needs policies to ensure that staff members are aware of their responsibilities. This includes extensive training for staff, and the creation of security and privacy champions within organisations that will review audit trails, and monitor for compliance with policies. Of course these are more challenging within resource-constrained environments,[48] but these responsibilities can be combined with other management initiatives.

The 'normative' regard for privacy and security within the medical profession is an essential safeguard that must be adequately sustained. It is essential that medical schools continue to ensure that medical students are trained in ethics and confidentiality. We were heartened to discover that a number of schools in Africa and Asia include lessons on confidentiality, but the material is in need of updating to consider the latest technological developments and attendant privacy and security risk dynamics.[49]

---

[47] 'Never heard of it - Understanding the public's lack of awareness of a new electronic patient record', Tanja Bratan et al., Health Expectations, 13(4): 379-391, December 2010.

[48] 'Policy Management for E-Health Records', Maritza Johnson & Steven M. Bellovin, HealthSec 2010, Usenix Security Workshop. Available at: http://www.cs.columbia.edu/~maritzaj/publications/2010_healthSec_position.pdf

[49] See 'Online Posting of Unprofessional Content by Medical Students', Katherine C. Chretien, S. Ryan Greysen, Jean-Paul Chretien, and Terry Kind. JAMA, 302(12): 1309-1315, 2009. Available at: http://jama.ama-assn.org/cgi/content/abstract/302/12/1309

Even the best policies and the best auditing techniques will still fail. Audit logs may be audited regularly but this must be done at the local point of care where abuses can be more clearly identified. Staff members may be authorised to access a file and yet may be abusing their rights of access nonetheless.[50] Accredited organisations may not appropriately enforce their policies and even if all the techniques are in place, it would still be very difficult to verify any wrongdoing.[51]

One of the most promising developments in eHealth for the protection of privacy and security of information is the opportunity for giving patients control over their information.[52] There are two emerging solutions to the challenge of patient empowerment. First is the use of 'locking' where patients' may choose to have their medical records locked or sealed and only used in very specific circumstances. This would mean that every access to the record would require the consent of the individual or an exceptional note on the log. Second is the empowerment of the individual to allow him or her to gain access to the audit logs to better understand how the patient records are used, thus forcing a degree of transparency on the healthcare organisation. Both of these approaches help to manage the consent of the patient, and would help patients set their preferences, access their own information, receive breach notification alerts, request that errors can be corrected, and make informed decisions about the secondary use of the information.[53]

Access controls and Training?
Results from one interview:
"In one hospital environment with around 500 members of staff, each member of staff had a unique account, there was a detailed policy framework for privacy and security, each member of staff was trained extensively about security and privacy issues in healthcare, and there was a thorough auditing system in place. Every year additional training would take place to remind them of their obligations about privacy and security. The hospital had a full time member of staff on security and privacy issues.

Even still, on average 5 people a year were disciplined for wrongfully accessing medical information."

---

[50] For a good example, see the results of the Investigation Report for the Office of the Information and Privacy Commissioner of Saskatchewan, where staff members of an accredited institution gained unauthorised access to patient files: 'L&M Pharmacy Inc., Sunrise Regional Health Authority, Ministry of Health', Report H-2010-001, March 23, 2010, available at http://www.oipc.sk.ca/Reports/H-2010-001,%20March%2023%202010.pdf

[51] See for instance, 'Order HO-002 from the Information and Privacy Commissioner of Ontario' regarding The Ottawa Hospital', July 2006, available at http://www.ipc.on.ca/images/Findings/up-HO_002.pdf

[52] See 'The Promise of Personal Health Records: A Resolution of Canada's Privacy Commissioners and Privacy Enforcement Officials', September 9-10 2009, available at http://www.priv.gc.ca/media/nr-c/2009/res_090910_eh_e.cfm

[53] See 'Use of Data from the Electronic Health Record for Health Research – current governance challenges and potential approaches', Donald J. Willison, commissioned by the Office of the Privacy Commissioner of Canada, available at http://www.priv.gc.ca/information/pub/ehr_200903_e.cfm

Opportunities for Securing Medical Privacy and Health Information

Even if we were to deploy eHealth systems in developing countries and emergency situations with the same safeguards we are developing for systems elsewhere in the world, there would remain significant challenges. The environmental and cultural differences are vast, even within a given country. We therefore need careful consideration and planning on the ground even as we devise policies and strategies at the national, regional, and international levels.

One of the ideal mechanisms for ensuring that privacy and security is through the infrastructure providers: the key implementing partners, the international organisations and community, and the funders.

Implementing Partners

At the earliest of stages, eHealth systems need to be designed with privacy and security in mind. This would require implementing partners to hold discussions on privacy and security as part of the early processes around devising a new system. This could be done as part of eHealth readiness assessments.[54] Adding privacy and security at a later date is insufficient as vulnerabilities will exist, inconveniences will be avoided, and it will be nearly impossible to impose principles of data minimisation. Enabling this will require the use of risk assessments, including privacy impact assessments.[55]

We must also ensure that local educational and training programmes are continued throughout the life-cycle of a project. All institutions and their staff that interact with the eHealth systems need regular training regarding privacy and security issues, and the attendant concerns about responsibility, accountability, and transparency. Each institution needs security and privacy staff members who can administer the appropriate privileges and maintain oversight mechanisms including audit trails.

International community

The international community must provide leadership in this domain and share the best practices from around the world. We are heartened to hear of interesting initiatives within industry to

[54] Cf. 'e-Health readiness assessment tools for healthcare institutions in developing countries', S. Khoja et al. Telemed J E Health, 13(4): 425-31, 2007.

[55] See, for instance, 'A Conceptual Privacy Impact Assessment on Canada's Electronic Health Record Solution', Blueprint Version 2, Canada Health Infoway, February 12, 2008; as well as 'Privacy impact assessment in the design of transnational public health information systems: the BIRO project', C T Di Iorio et al., J Med Ethics, 35: 753–761, 2009.

develop best practices and even standards on privacy and security. Similarly, international organisations are in an ideal position to promote discussion and consideration of these issues. The WHO's planned work on developing thought-leadership on patient identifiers is also a promising development.

Funders

The funders of these projects and initiatives have the heaviest responsibility in ensuring that their projects are fit for purpose. The worst case scenario must be avoided: an eHealth system that increases access to healthcare to vulnerable people while making them vulnerable to abuse through weak privacy and security controls. A false sense of security is a great breach of trust and confidence.

Funders must do far more than they are doing to date, by requiring partners and grantees to conduct assessments and consider these ethical issues at the outset. Resources will also be required for regular audits and subsequent follow-up work. Privacy and security are processes, not products or plug-ins.

Funders must also consider law and policy change as an integral component of the deployment of a new system and practices. They should promote legal rights and effective regulatory controls and accessible rights of remedy even before the systems are specified.

Next steps

As we move forward in the eHealth privacy and security space, we aim to assist these actors in these efforts by:

- engaging with the international health community (e.g. WHO, ICRC, etc.) to identify the most pressing dimensions of eHealth privacy and security;
- further engaging with the funding bodies that make eHealth systems possible in developing countries and humanitarian and relief operations;
- continuing our engagement with technology developers and experts in order to assist in the design and implementation of privacy-friendly and secure health information systems;
- developing detailed case studies to increase the knowledge base in this area;
- developing recommended content coverage for ethics courses in medical schools in developing countries; and
- developing recommended policy frameworks with which to guide future decision-making.

Concluding remarks

There are times when the interests of the funders, international community, and implementing partners will conflict with the issues that we have raised in this report. There will also be times where conflicts will arise between each community, or even within each community. This is a sign of a healthy discourse about technology and policy.

These disagreements will occur particularly when these communities are all acting in the best interests of the patients and citizens. These disagreements may be about data-sharing for health surveillance, reporting in order to understand programme effectiveness, using information for accounting to manage costs, or accessing information for medical research. These same debates occur around the world and we must always recall that a well-rounded debate is necessary in order to have a healthy discourse.

The challenge for developing countries and humanitarian operations is that we have a tendency to think and act on behalf of the citizens and patients. At times like these we must remember that underlying everything we are doing and all the issues raised in this report is a fundamental understanding within the practice of medicine that we are here to protect the rights of humans.

Annex

Workshops and consultations:

Date	Location	Title of Event	Objectives	Types of Participant	Our participation
July 2010	London School of Economics, London, UK	Workshop on Medical Privacy in Developing Countries	Initial scoping exercise with UK-based experts	Experts in medical informatics and privacy	Workshop co-ordinators
August 2010	Washington, DC, USA	1st USENIX Workshop on Health Security and Privacy (HealthSec '10)	Computer science workshop on health information security	Primarily technical experts in medical and health security and privacy	Audience members
September 2010	Cape Town, South Africa	Fifth Annual OpenMRS Implementers Meeting	Annual meeting for the OpenMRS community to share their experiences	OpenMRS developers and implementers	Presentation on privacy aspects of e-health; interviews with workshop attendees
September 2010	Cape Town, South Africa	13th International Congress on Medical Informatics (MedInfo 2010)	Annual conference of medical informatics community	Health practitioners, academics, policy makers	Attended conference presentations; interviewed experts at conference
September 2010	St Hugh's College, University of Oxford, Oxford, UK	International Data Sharing Conference	Multi-disciplinary meeting to share ideas for and experiences of health and biomedical data sharing	Public health researchers and biobanks experts	Presented preliminary research findings

Overview of the types of reviewers of our draft documents:

Specialization	Geographic Region
Medical law	Africa
Health practitioner	Africa
Health information systems	Asia
Health practitioner	Asia
Data protection	North America
Health information security	North America
Health information security	Europe
Health information management	Europe
Medical privacy	Europe
Medical informatics	Europe
Information privacy	Europe