INFORMATION SYSTEMS
AND INNOVATION GROUP
Department of Management

Research Note

Privacy and Security of Medical Information in Developing Countries and Emergency Situations:

Broadening the Threat Model

PEN paper 6, May 2010

Privacy and Security of Medical Information in Developing Countries and Emergency Situations by Dr. Gus Hosein and Aaron Martin

As we move forward with the development and deployment of digital health information systems we must consider their eventual use in legally problematic and perhaps even hostile environments. These systems are being deployed at great speed in developing countries and emergency situations where there is limited informed deliberation and debate. In turn, there are few considerations of information security and privacy.

We are concerned that international aid agencies and governments are introducing new risks and dangers that may conflict with the noble goals of providing medical care in developing countries and emergency situations. It is essential that the technical and policy research communities consider these realities as we develop our use cases, risk strategies, and threat models.

Developing Countries and Emergency Situations

Digital health information systems have great potential to enhance healthcare in developing countries and to provide care in emergency situations. Aid can be disbursed in ways that were previously unimaginable, saving lives and enhancing the quality of life for millions. Advanced techniques and devices may soon be deployed to enable healthcare to be provided through mobile communications and platforms to environments with limited technological resources, and to permit the collection and management of health information across borders. Concurrently, new techniques are being adopted for the surveillance of transmittable diseases such as malaria, so as to better understand disease vectors and in turn develop better containment policies. This is why 'eHealth' is receiving substantial attention from development funding agencies.

Yet governments, funding agencies, and international organisations rarely consider privacy in their designs. Our experiences from working on information security and privacy issues within international organisations such as the UN Refugee Agency (UNHCR) indicate that even the most basic privacy and security safeguards are not easily adapted to resource-constrained environments, be they refugee camps, emergency situations, or developing countries.

Legal and regulatory resources that we take for granted in more developed scenarios are unlikely to be adequate to protect the interests of patients. The omission of data security and privacy is certainly not without reason: flexibility and usability are key specifications and requirements for systems used in less technologically rich domains. Security models are often distant concerns as professionals focus on the delivery of systems, sometimes using the most basic technologies that were never intended for these purposes (e.g. using Microsoft Office applications as medical information databases). As resources are limited there may be a temptation to share information with third parties to ensure that these initiatives become sustainable.

Medical information can be used to place individuals in grave danger in these environments. Medical histories can be used to discriminate or target specific groups or individuals. Yet information often goes missing, and is shared without regard to due process. Neither the technological preventative measures nor legal rights of recourse are offered to individuals. Audit logs are not available to track access and use, so individuals are never notified that a breach has occurred.

Research Questions

With the attention of funding agencies focused on the deployment of the state of the art, this is our opportunity to assist them in considering privacy and security. We are working with international development organisations to devise an analytical framework for evaluating how prospective projects consider privacy and security risks.

At this early phase in our research, we are approaching this problem space by focussing our attention on:

Building legal responsibilities and rights. Collecting and using health information often hinges on consent of the patient, but the qualification of consent is context-dependent. For instance, we have seen the deployment of systems in refugee camps where if refugees refused to hand over information they risked losing access to services. Can systems designers help ensure that even in the absence of informed consent, information is appropriately secured?

Regulating access. In some environments, inappropriate access to medical records can result in persecution, or worse. Following on the case of *I v Finland* where the European Court of Human Rights ruled that inadequate security over information about one's HIV status was in breach of human rights law, we need to imagine the ramifications of such breaches in more hostile environments even as the collection and use of this information is integral to healthcare. What are the best practices for managing information collection, access, and storage?

Auditing use and sharing. To what purposes can health information be put to use, apart from serving the immediate interests of the patient? Cases from around the world show that once collected, other parties are interested in gaining access to health information, including government agencies, political campaigns, insurance companies, pharmaceutical organizations, civil society, and health researchers. There is no concerted initiative to monitor the contractual arrangements on the limitations of use and sharing of this information as health IT systems are deployed worldwide. Is it possible to devise provable means of limiting the processing of personal information, particularly in environments where the users and patients are not aware of their own rights?

Objectives

We aim to bridge the communications gap on privacy and security between designers, researchers, users, as well as policy-makers so that they are attentive to the risks and challenges of pursuing eHealth initiatives in developing countries and emergency situations:

- We will work with eHealth workers in the developing world to understand what is driving the deployment of new systems; what are the risks, limitations, and constraints in their environments; and to help identify opportunities to enhance the security and privacy of medical information.
- We will also consult designers, implementers, and other technologists to understand what is technologically possible, so that we can inform project managers in developing countries and emergency situations of their options. In turn we hope to advise the technological community of the risks to designing their products without considering the developing world environment. That is, we aim to inform the technologists of the challenges in developing countries and emergency situations, to consider them in future threat modelling, use cases, and risk assessments.
- We also hope to appeal to policy-makers by identifying the best available techniques for security and privacy of medical information.

Finally, we also hope that this work will be of interest to the wider development community. While there is a significant amount of investment in eHealth because it is compatible with the development agenda, it may conflict with the human rights agenda; i.e. systems that leave processing open to abuse are likely to breach rights. By researching how these two agendas can be resolved with one another, we may be able to set a precedent for the development and human rights communities at large.

This work is being carried out with the aid of a grant from the International Development Research Centre, Ottawa, Canada.