Privacy Challenges in the Use of eHealth Systems for Public Health Management

Karpurika Raychaudhuri, University of New South Wales, Australia
Pradeep Ray, University of New South Wales, Australia

ABSTRACT

Privacy is a major issue in information management for public health needs. For example, the surveillance of infectious diseases, such as HIV, is an important function of public health and it presents major privacy concerns for affected people. While their privacy must be protected, privacy concerns should not come in the way of effective data collection and surveillance. In this paper, the authors present a survey of published work covering privacy challenges in the use of eHealth systems, especially in the context of public health management. The authors identify and present the major privacy challenges, their effects on personal patient privacy and public health management based on the review of research in electronic data privacy and eHealth privacy. The authors also present a survey of privacy-preserving technologies and solutions that address these challenges.

Keywords: Anonymity, Data Mining, eHealth, Privacy, Privacy Challenges, Public Health, Surveillance

INTRODUCTION

Advances in information and communication technology have provided new opportunities for enhancing existing health care infrastructure to reach wider segments of national populations, and have made eHealth systems very attractive for the purposes of public health management. Amidst threats of bio-terrorism, attacks such as the Anthrax scare, pandemics such as HIV/AIDS, avian influenza, the swine flu and natural disasters like hurricanes and tsunamis, public health preparedness has become an important issue worldwide. Additionally, there is also concern over ageing populations and their related health care costs in certain countries like Australia, Japan, and the European Union, including France and Germany.

Privacy is a major concern of the population, particularly if there is stigma associated with the illness (e.g., HIV/AIDS). Although the information technology is being extensively used in healthcare industry, there is a lack of robustness in these health information systems from the perspective of privacy management as exemplified by this case: A California-based company, Health Net which insured about 2.2 million people, mailed a list of patient’s names being treated for depression with associated anxiety erroneously to nearly 5,000 physi-

DOI: 10.4018/jehmc.2010040102
In order to achieve widespread adoption of eHealth (healthcare based on information and communication technologies) systems, every patient should have and be able to control their own electronic health record with a provider of their choice. People should also be able to approve health care providers and caregivers to have access to their records. However, legislation changes continue to be debated and discussed to ensure the privacy of electronic health data is preserved, more so, when used for purposes other than primary patient care. While eHealth systems offer many benefits that will help improve the quality of private and public healthcare, their use must be balanced with user privacy and security concerns in order to make the systems socially and politically acceptable.

In light of this very topical issue in eHealth, the goal of this report is to review academic and practice literature, analyse the findings and report on the following.

a. What are the major concerns about patient privacy of eHealth data used for purposes other than primary patient care? How do these privacy concerns affect public health management initiatives?
b. How do privacy legislation and government policies on eHealth regulations address these challenges?
c. How do privacy-preserving tools and technology solutions address these challenges?

This paper is organized as follows: first, we briefly discuss the background of privacy and public health surveillance. This is followed by an overview of the major privacy challenges for eHealth systems in the context of public health management. We then discuss how existing privacy legislation addresses the privacy challenges followed by an overview of privacy-preserving technology solutions.

PRIVACY AND PUBLIC HEALTH SURVEILLANCE

‘Privacy’ is a common word having many connotations. The Oxford English Dictionary defines privacy as “a state in which one is not observed or disturbed by others” (Henderson, 2006). In more recent times of the internet and information technology era, it has come to mean the loss of control of personal information, generally because of technology. Preservation of privacy is becoming more challenging as a result of information technology advancements. Privacy of personal electronic data is an issue that extends beyond the eHealth domain. Research addresses general privacy and security concerns related to personal information in electronic systems (Moloney & Bannister, 2008), not just eHealth, including collection of, unauthorized use of, improper access to, errors in, and purpose for collection of personal information.

Privacy is held to be valuable because it is believed to protect individuals from all kinds of external threats such as defamation, harassment, manipulation, blackmail, theft, subordination and exclusion. Privacy is an articulation of the core value of ‘security’, meant to protect people from all kinds of harm done by others (Moor, 1997). In most industrialized nations, the right to privacy is considered a fundamental human right (Fried, 1990). Privacy is valued in modern societies who also value the ideal of the autonomous individual. Yet modern society is also characterized by ‘Surveillance’, which is the systematic observation of people groups for specific purposes (Petkovic & Jonker, 2006).

In the 1960’s and 70’s, the public debate over privacy surfaced when governments started surveying their countries population. Privacy debate resurfaced when computers appeared and the right to data protection emerged. Today, advances in IT has made possible surveillance to be done on large scale computerized data collection, and processing of personal data in order to monitor peoples actions and communications (Petkovic & Jonker, 2006). Massive collection of personal data and ubiquitous...
The Implementation of Cloud-Based Telemedical Applications for External Quality Control Purposes in the Field of Cytopathology