Privacy Controls for Electronic Health Records Systems

Tyrone Grandison PhD
Data Disclosure Research, Healthcare Informatics Department
IBM Almaden Research
San Jose, USA
tyroneg@us.ibm.com

ABSTRACT

The federal push to have the US healthcare system completely electronic in the next decade raises significiant challenges to Information Technology professionals tasked with the job of implementing these systems and ensuring that they work properly. The obvious technical issues of storage medium representation and optimisation, appropriate security models and systems interoperability will eventually be solved and can be driven by the needs of practitioners, patients and payers. However, one of the primary deployment deterrents, i.e. the privacy of information in an Electronic Health Record (EHR), involves not only business, social and technology factors, but also legislative factors. This conglomeration of factors may lead to multiple technical solutions with divergent assumptions. This presentation examines those alternatives and advocates a system amenable to patient empowerment.

1. INTRODUCTION

In legislative circles, an invasion of privacy has been long thought of as an infraction of the bounds of one's physical space, i.e. one's home. With the advent of the telephone, and then the Internet, this well-defined boundary has been significantly blurred, and is slowly leading to a re-evaluation of the legal viewpoint on privacy compliance. The prevailing belief system ushered in an era of *active compliance*, where technical solutions that facilitate privacy compliance focus on enforcing compliance rules at the point of data collection or data access. This promoted the notion that enforcement of privacy rules is possible in real-time at the front end of transactions. This has created a burdensome systems management concern as the number of applications and privacy directives increase. Both of these issues imply that the fundamental technical privacy concerns to be addressed are: the location of privacy controls used in EHR applications, and the point of operation/enforcement of the technology.

2. LOCATION OF PRIVACY CONTROL

At its most basic, an EHR system should be viewed as a singular unit of information belonging to a patient. Whether storage mandates dictate that various elements are spread across healthcare entities or not is irrelevant. Conceptually, the EHR is per patient and can only be unlocked with his or her consent. This implies that segments not directly under the patients' control should automatically abide by the patients wishes. Thus, the placement of the mechanism that enables this assurance is crucial in providing the patient with a true measure of compliance with his privacy wishes. The options are: around the EHR system or sub-system, in the operating system or in the healthcare applications. Each of these choices have significant ramifications on the usability, interoperability and scaleability of the EHR system. These alternatives will be discussed further in the presentation and the impacts of each outlined.

3. POINT OF ENFORCEMENT

The current state of the art in privacy enforcement assumes that it is possible to prevent circumvention of compliance before an incident occurs. Unfortunately, the current state of vigilance and concern when it comes to proactive monitoring of privacy statements and adherence to them, by patients, is very low. This is due to a multitude of factors; one being the mental load required to understand the umbrella declarations in these statements, which are normally written in legalese. Thus, consent to *active enforcement* at data creation and access times is nebulous in value in the eyes of the patients; as he or she is unsure of what this enforcement means.

It is also the case that information goes through several steps in its lifetime (Fig.1). Performing enforcement at collection and access will only address concerns at two specific points. There will still be issues as other processing takes place.

Figure 1: Information Management Lifecycle

This leads to a discussion on the type of controls needed when information is shared, stored offline or offshore, published, etc. Policies will need to stick to data throughout its lifecycle and information needs to be kept efficiently and comprehensively in order to abate any complaints that a patient may have in future. Thus, one can either actively enforce at the application front-end, or enable sticky policies that are enforceable at each stage of the information lifecycle or collect enough provenance data to ensure that accountability is built into the system. One or all of these approaches may be employed. However, each place demands on the overall system infrastructure and has particular imperatives that may make them infeasible for Electronic Health Records.

4. THE PROPOSAL

After an evaluation of the alternatives, their underlying assumptions and potential ramifications, I propose a EHR wrapper-based solution that optimally stores provenance information that can be proactively analysed for privacy incursions.