Cryptology ePrint Archive: Report 2011/016

An Anonymous Health Care System

Melissa Chase and Kristin Lauter

Abstract: As medical records are converted to electronic form, risks of compromise of patients' privacy increase dramatically. The electronic format makes misuse of many patients' data much easier, so we must be extremely careful with who has access to this data. At the same time, this move to an electronic approach also gives us opportunities to improve patient privacy by leveraging recent cryptographic techniques, and in some ways to improve upon the traditional system.

Here we look in particular at those parties, such as insurers and pharmacies, that are not actively involved in patient care. Currently patients who are insured are required to share the entire record of their medical treatment with their insurer in order to receive benefits, and a pharmacy may store all prescriptions filled for each patient.

However, there is no medical reason for these parties to see this information --- they only need enough information to be able to prevent fraud and verify that the provided treatment should be covered under the patient's policy, or that the patient has a valid prescription for the medication being dispensed. We argue that, using recent developments in cryptography, we can allow this verification without revealing any additional information about the patient's record, thus obtaining optimal privacy guarantees.

Category / Keywords: applications /

Publication Info: presented at HealthSec '10

Date: received 7 Jan 2011

Contact author: melissac at microsoft com