Utilizing Smart Cards for Authentication and Compliance Tracking in a Diabetes Case Management System

Michael K. Baldwin
Department of Computer Science
Tennessee Technological University
P.O. Box 5101
Cookeville, TN 38505, USA
mkbaldwin21@tntech.edu

Brandon M. Malone
Department of Computer Science
Tennessee Technological University
P.O. Box 5101
Cookeville, TN 38505, USA
bmmalone21@tntech.edu

ABSTRACT

This poster describes the use of smart cards for patient authentication and real time compliance tracking based on a physician prescribed treatment plan, in a diabetes case management system.

1. INTRODUCTION

There have been many medical record systems developed which utilize smart card technologies for various aspects of the system from authentication to record storage [2]. This poster documents a new system which utilizes smart cards in a new way to provide patient authentication and real-time compliance tracking for diabetes case management.

Smart cards are small plastic cards, about the same size as a credit card, that contain a small embedded microchip. The exact dimensions, electrical properties, and communications protocols are defined by the ISO 7810 standard [4]. The microchip can contain either memory only, i.e. a memory card, or both a microprocessor and memory, i.e. a processor card. The memory capacity of the cards can vary from as small as a few hundred bytes to many thousands of bytes.

The cards selected for use in this system are processor cards with a storage capacity of approximately 22KB. These processor cards were chosen over less expensive memory cards due to a limitation of an existing, commercially available, ActiveX control that is used to allow for interaction between JavaScript code in the browser and the card reader.

2. SYSTEM OBJECTIVES

The primary objectives of this system are to improve diabetes case management and reduce or prevent fraudulent claims by providers, by utilizing smart cards and a newly designed web application.

ACM-SE '08, March 28–29, 2008, Auburn, AL, USA.

2.1 AUTHENTICATION

Along with case management functionality the system also allows the patients to pay for various services, related to their diabetes care, by filing claims using their smart card. When a patient visits a participating provider they will present their smart card. When the card is inserted into a reader a header field, containing authentication information, is read and sent back to the server via an AJAX request. Once the header has been processed on the server the provider is presented with a photograph of the patient for manual verification and is prompted for the patients PIN. Once this information has been entered another request will be made to the server. Upon verification the provider will be presented with a page which allows for claims to be filed for the patient whose card is in the reader.

This prevents a provider from filing claims for services unless the patient is present in the office by utilizing the smart card as a part of a two-factor authentication scheme. In our case the smart card acts as the first factor of authentication (something they have) while the subsequent entry of a PIN number provides a second factor (something they know) [1]. This is a system which is already familiar to anyone who has ever used a debit card.

2.2 CASE MANAGEMENT

The primary goal of any case management endeavor entails ensuring patients follow an effective prescribed treatment plan [3]. Especially for some high-risk demographics, such as diabetic patients, some simple case management can prevent serious complications like peripheral neuropathy or loss of vision. Other advantages of a case manager include encouraging patients to comply with their plan, as well as functioning as a conduit of communication between the patient and physician between office visits.

While many different segments of the population can benefit from case management, such as diabetic patients, drug offenders, etc., these divers demographics demand differing treatment plans. The physicians of the diabetic patients under study supplied their plans, which include activities such as "visit the gym three times per week", "receive an A1C test three times per year," etc. Once the physicians provide the treatment plan, the case manager schedules appropriate appointments for the patients with providers, such as the gym, hospital, etc.

In order to ensure the patients follow the treatment plan defined by their physicians, smart card readers installed at provider locations allow patients to swipe their cards. After swiping the card, the provider indicates the services performed. Comparison between the services provided to the patient and the physician-defined treatment plan determines the compliance of the patient.

In addition to tracking whether patients follow their prescribed plan, case management also concerns itself with verifying the effectiveness of the plan. Hence, the system also monitors outcomes data, such as weight, blood pressure, and A1C lab results. The case manager inputs these results into the system. The case manager typically receives this data via fax from testing facilities, such as the gym for weight and blood pressure and the hospital for A1C results.

Because the case manager has many responsibilities, including contacting providers to schedule visits, tracking the compliance of the patients to their plans, and monitoring the outcomes of the patients' labs, the system must present this data in an intuitive, easy-to-view fashion. Partitioning this information into easier to digest portions ensures the volume of data does not overwhelm the case manager. A first view of the data lists all of the patients not in compliance with their treatment plan, either because the case manager needs to schedule a visit for the patient or because the patient has missed a visit. An alternative view lists patients based on the results of their lab tests.

After the case manager identifies that a patient requires attention, her next actions depend on the specifics of the patient's case. If a patient needs an appointment, the case manager schedules the appointment and alerts the patient. When a patient misses an appointment, the case manager contacts the patient to ensure he or she realizes the missed appointment. The case manager then reschedules the appointment. Finally, for poor lab results, the case manager alerts both the patient and the physician of the patient that the current plan may need adjustment.

3. CURRENT STATUS

As mentioned earlier, the current system implementation employs an encrypted integer identifier to authenticate patients to the system. Additionally, a four-digit PIN provides a second factor for authentication. Currently, patients can choose from local network of providers who have smart card readers installed at their place of business. The system can only track services patients receive at these locations. At present, lab results indicating the outcomes of following the treatment plan are introduced into the system via a form in the interface. The case manager manually inputs results faxed, or otherwise transmitted, to her.

In order to boost the security of the authentication mechanisms, a stronger key, such as some sort of GUID, could authenticate the patient to the system. While the diabetic patients can currently acquire nearly all of the services necessary to treat their disease, they rarely have more than one or two options for any given service. For example, patients can only visit the gym to work out; the system could not track a patient's visits to a pool to swim laps. An expanded provider network would grant the patients more options.

Nearly all of the providers involved in administering labs input the results into their own EMR system. Automatic entry of these results into the system could reduce the workload of the case manager.

Especially in America, smart cards are still an emergent technology looking for a home. The implemented system demonstrates that smart cards can play a role in multi-factor authentication, as well as tracking activities at known locations equipped with proper hardware and software.

4. ACKNOWLEDGEMENTS

This work was funded by Tennessee Technological University and the Tennessee Department of Finance and Administration to study the feasibility of the use of Smart Card technology in state government. This publication has not been approved by the Tennessee Department of Finance and Administration.

5. REFERENCES

[1] CardLogix. Two-factor authentication for internet transactions. WhitePaper, 2004.

[2] Fulcher, J. The use of smart devices in ehealth. In *ISICT '03: Proceedings of the 1st international symposium on Information and communication technologies* (2003), Trinity College Dublin, pp. 27–32.

[3] Paula M. Trief, PHD, Jeanne A. Teresi, EDD, PHD, Roberto Izquierdo, MD, Philip C. Morin, MS, Robin Goland, MD, Leslie Field, RN, MSN, Joseph P. Eimicke, MS, Rebecca Brittain, BS, Justin Starren, MD, PHD, Steven Shea, MD, and Ruth S. Weinstock, MD, PHD. Psychosocial outcomes of telemedicine case management for elderly patients with diabetes. *Diabetes Care 30*, 5 (May 2007), 1266 – 1268.

[4] Rankl, W., and Effing, W. *Smart Card Handbook*. John Wiley and Sons, 2003.