Lockstep Babysteps No. 6

Smartcards and healthcare provider fraud

Health & welfare smartcards have special potential advantages for combating provider fraud, especially in offline environments where points of service are not connected to central mainframes. There are valuable lessons for health cards arising from the EMV[1] smart credit card programme, where abuse of lost and stolen cards is better detected and managed across a wide range of offline settings. Some of the finance sector's concerns over card abuse translate into the health & welfare sector, and show how to combat provider fraud, over-servicing, prescription shopping and so on.

This paper looks at bogus claiming perpetrated by corrupt providers, clinic administrators and government clerks.

Lessons from smart credit & debit cards

The EMV programme represents a comprehensive attack on card fraud, with significant lessons that are applicable to health & welfare. While smartcard security is usually thought of in terms of immunity to skimming and counterfeiting, the full range of anti-fraud measures in EMV has more to do with the intelligence and multi-programmability of smartcards.

One of the key strengths of smartcards is their ability to *keep tabs on transactions and to enforce transaction caps without terminal equipment having to go online to backend mainframe databases.* A smartcard can automatically detect when a daily limit has been reached, and flag the fact to the terminal. More sophisticated business rules can be programmed, including the use of different thresholds in different locations, such as designated high risk outlets, or overseas (where daily caps might be raised temporarily to allow for heavier spending during travel). All these types of rules are enforceable by the smartcard itself while offline, thus dramatically improving fraud protection across traditionally difficult retail environments where connections to backend systems cannot be guaranteed.

Application in health & welfare

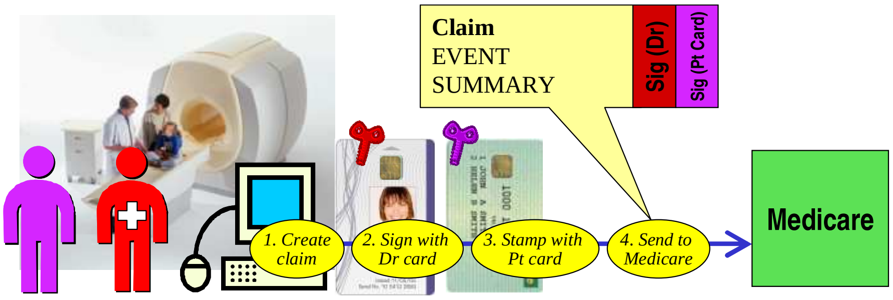
Smartcards can autonomously enforce all sorts of entitlements rules and "reasonableness tests" – not just financial ones. Primary healthcare in Australia covers a notoriously diverse range of locations, including suburban surgeries and pharmacies, rural & remote practices, base hospitals, community care, mobile public health screening units, and mobile out-patient clinics. It is often prohibitively expensive or outright impossible to connect to backend data-bases for real time fraud monitoring. Furthermore, *centralised monitoring of every single transaction in order to weed out a tiny minority of fraud cases jeopardises the privacy and security of the vast majority of law abiding users.*

Smartcards can directly address two major forms of Medicare fraud:

1. ***Prescription shopping***, where a patient sees a number of different providers in quick succession to obtain drugs or some other benefit, can be detected by the card without transmitting sensitive data over the network, by checking e.g. the time between doctor visits, or the number of scripts written in a period (see *Babystep 7*).
2. ***Fraudulent claiming by providers*** for item numbers not actually delivered, or the counterfeiting of claims by administrative clerical staff.

Reducing provider fraud

The diagram shows an un-forgeable, indelible virtual stamp – *Sig(Pt Card)* – created using an embedded key specific to the patient card, and attached to the event summary. For a claim to be legitimate, it would have to feature both the digital signature of the doctor ordering the item, and the stamp corresponding to the patient. Counterfeit claims could not be created without collusion with the patient and access to their particular smartcard. Over-servicing would be readily detected if the same patient card was seen to be associated with multiple claims.



[1] EMV stands for *Europay-MasterCard-Visa*, the founding members of the standards consortium of credit card companies.