A new way to safeguard health IDs against theft and abuse

Executive Summary

Electronic Health Record use is growing worldwide. Highly elaborate (if problematic) government systems feature in many countries, while diverse Personal Health Record (PHR) services are booming amongst HMOs, government agencies, large employers, online social networks, and as start-up commercial offerings. Many policy makers believe EHRs and PHRs are crucial for future patient centred care models, better health outcomes and improved healthcare efficiencies.

The basic right of patients to access their own records is recognised in most places, yet the current state of user authentication puts PHR users at enormous risk. Conventional username-and-password logon leaves users utterly vulnerable to ID theft, phishing and pharming (where users are drawn to what appears to be a legitimate PHR website but which is in fact a criminal enterprise trying to elicit their personal details).

To date, little attention has been given to the protection of health identifiers against theft and replay attack. Alphanumeric health IDs are prone to the same sorts of attack that are plaguing retail payments systems. Discovering a person's identifier (or credit card number) and then replaying it without their possession is child's play. "Card Not Present" fraud is the fastest growing form of financial fraud, accounting for at least $5billion in losses annually worldwide. It is hardly surprising that the analogous problem of Medical Identity Theft is already escalating.

The lesson for healthcare systems is to pay attention not only to access control but also to the "pedigree" of identifiers. Service providers, especially PHR operators, must be certain that every given health ID really pertains to a singular individual, and that it has been presented voluntarily each time the service is accessed. In particular, health IDs as authenticators must not be replayable. Yet despite the prevalence of identity theft, health ID standards work (such as the ASTM *Standard Guide for Properties of a Universal Healthcare Identifier and* the HIPAA security rule) have had nothing to say about the unauthorised use of IDs.

The inattention to health ID security is a significant policy shortfall. In the financial services sector, authentication is a priority issue; simple password access to Internet banking is already superseded. The health sector surely needs to not only catch up with online banking security but go one step better, for the risks are so much greater. There is probably no worse privacy breach than having ones identity stolen and health records exposed; unlike money, the loss of health information cannot be readily compensated. So PHRs and other e-health services should adopt not just two factor authentication but *non-replayable* authentication of patients as well.

Lockstep Technologies' award-winning *Stepwise* security and privacy solution safeguards personal identifiers with smart ID devices. *Stepwise* can greatly enhance de-identification and patient confidentiality, and cut Medical Identity Theft. This paper describes the solution, and sets out a detailed proposal for how it can be deployed in scaleable e-health settings, using the exemplar of a clinical trial.

Background: Lockstep Technologies' *Stepwise*

Stepwise securely encapsulates individual identifiers and seals them cryptographically into an individual's smartcard or similar security device. *Stepwise* isolates each identifier, removes all extraneous personal detail and linkages, and ensures that when any identifier is presented online, we can be confident that it is legitimate and that has been used with consent. *Stepwise* prevents an identifier from being stolen and misused without permission. By enhancing the pedigree of personal IDs, *Stepwise* also allows extraneous identifying information to be stripped away from e-health transactions, dramatically improving de-identification and privacy. The benefits of *Stepwise* include:

- IDs cannot be cloned, counterfeited, or illicitly copied
- every transaction bears a tamper-proof pedigree, proving it originated from an authentic personal security device carrying a bona fide identifier, used with the consent of the owner
- because all data records are sealed and de-identified, the integrity and traceability of data, and the confidentiality and privacy of individuals are all greatly enhanced.

Technically each *Stepwise* "capsule" is actually an anonymous digital certificate issued to a smartcard or similar device and holding an identifier such as a unique health ID. The capsule (certificate) links the identifier to the card, and permits transactions originating from the card to be sealed (digitally signed) with the identifier. For more information, see www.lockstep.com.au/technologies/stepwise.

Worked example: Using *Stepwise* to improve clinical trial data confidentiality

Huge amounts of highly sensitive data are gathered routinely during clinical trials as well as post market surveillance of pharmaceuticals, devices and so on. Anonymity and de-identification are critical; not only is patient confidentiality paramount, but assignments to treatment and control arms in double-blind trials must remain secret. Yet there must be dependable *indexing* of clinical trial data to ensure that records pertaining to individuals cannot be mixed up or altered, accidentally or otherwise.

The Lockstep Technologies proposal is to use smartcards and *Stepwise*-protected trial identifiers to manage the data from participants in clinical trials to enhance patient confidentiality and de-identify all data. The proposal introduces smartcard issuance and an additional layer of standards-based security to clinical trial software.

The following diagrams illustrate the concept. The setup of a clinical trial or surveillance program generally involves recruiting investigators and distributing information packs, protocol documents, company data collection software and, in the case of drug trials, treatment packs variously containing active agents and placebos. With the *Stepwise* solution, the study sponsor would also issue each investigator with a personal smartcard and smartcard reader.

Each subject will be issued with their own smartcard[1] when enrolled into the study, to carry their *Stepwise*-encapsulated trial ID. The patient smartcard would most likely be a sponsor-branded card[2] preferably handed out by the investigator, or else sent through the post. Sponsor-issued smartcards would generally be kept by the patient and presented at each follow-up visit.

With each new enrolment, the subject ID is sealed within a *Stepwise* capsule and loaded to the individual's smartcard. This can be done in real time when using existing health smartcards, personalising them on the spot via the investigator's card reader and software. *Stepwise* capsules are specially formatted digital certificates produced by a standard certificate server; sponsors can use an in-house server or an outsourced service, under a scheme such as the pharmaceutical industry's SAFE-BioPharma.

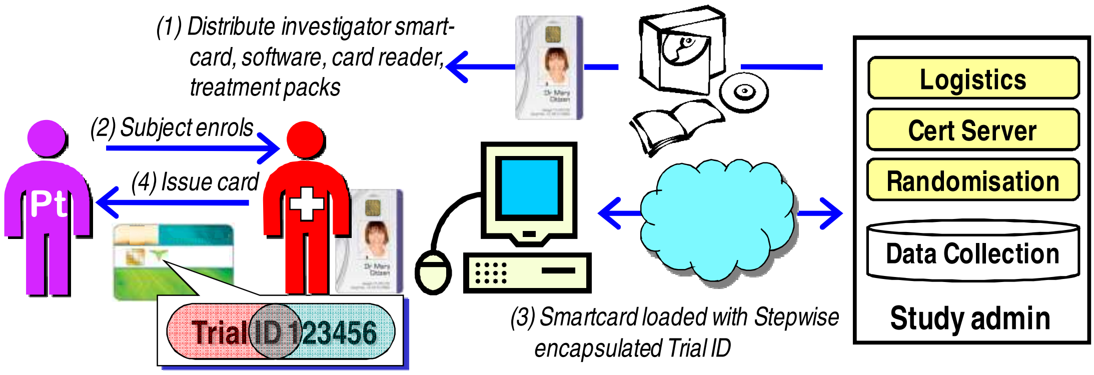
(1) Distribute investigator smart-card, software, card reader, treatment packs
(2) Subject enrols
(4) Issue card
Pt
Trial ID 123456
(3) Smartcard loaded with Stepwise encapsulated Trial ID
Logistics
Cert Server
Randomisation
Data Collection
Study admin

Figure 1: Issuing study subjects with *Stepwise*-protected IDs

At follow-up visits, the study subject presents their smartcard and their ID is retrieved by the software and validated through the *Stepwise* capsule. Test results and other data are collated as usual, uploaded to the study software application, and then sealed (digitally signed) using the *Stepwise* capsule and the subject's smartcard. All other personal information can be stripped from the clinical record, de-identifying it and enhancing patient confidentiality.

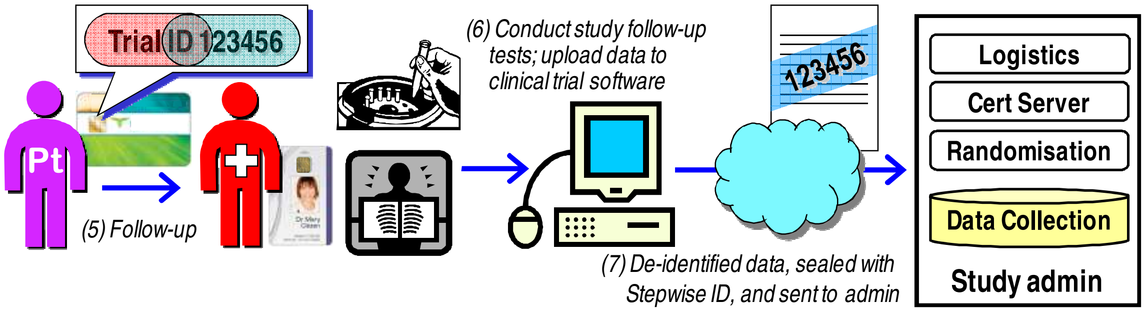
Trial ID 123456
Pt
(5) Follow-up
(6) Conduct study follow-up tests; upload data to clinical trial software
123456
(7) De-identified data, sealed with Stepwise ID, and sent to admin
Logistics
Cert Server
Randomisation
Data Collection
Study admin

Figure 2: Using *Stepwise*-protected IDs at follow-up visits

[1] Alternatively, *Stepwise* works just as well with other cryptographic media such as USB keys.

[2] Instead of sponsor-issued cards, *Stepwise* capsules can be loaded into many of today's multi-purpose government smartcards, such as the US Government Personal Identity Verification (PIV) card, the health cards of Austria, France, Germany, Slovenia and Taiwan, and the smart ID cards of Estonia, Hong Kong, Malaysia and Thailand.

Integrating *Stepwise* into clinical trial software

Stepwise is an entirely standards-based approach, using conventional multi-function cryptographic smartcards and digital certificate services. As such, *Stepwise* is fully compatible with common smartcard platforms and PKI schemes like SAFE BioPharma, the US Federal Personal Identity Verification standard FIPS-201, and Global Platform. In some settings (notably patients accessing the PHR from home), smartcards are not yet seamless to use, because they usually require a card reader to be installed. For these cases, *Stepwise* can just as well be implemented using plug-and-play USB crypto keys.

Integrating *Stepwise* into client or server components of existing clinical data management software is straightforward. Basic certificate management and digital signature software functions are required; these are commonly built into commercial platforms such as Windows, and are otherwise widely available in commercial or open source security toolkits.

Lockstep's *Stepwise* demonstrator – as featured on ABC TV in a Card Not Present payment configuration[3] – was built from off-the-shelf e-commerce server components with the addition of a just a few dozen lines of code. Programmers guides are available for the customisation of health data management applications.

Applicability to other healthcare settings

The worked example detailed above can be readily expanded into other settings:

- private sector or public sector EHRs in countries with multi-programmable smart health cards or suitable multi-purpose government ID cards
- outpatient PHRs at hospitals where smartcards are being used for in-patient ID
- clinical databases for armed forces personnel in e.g. Australia or the USA, equipped with Common Access Cards (CAC)
- employee PHRs in US government workplaces using FIPS 201 badges
- commercial PHRs with their own USB keys issued to users for security
- employee PHRs in private sector workplaces using multi-function smartcard badges for identity and access control.

Benefits of *Stepwise* in protecting health IDs

- Patient identities cannot be ascertained from their e-health transactions
- all e-health reporting is tamper resistant: every patient-specific transaction can bear an indelible digital seal validating the patient ID and proving that the ID has been held safe in a genuine authorised smartcard
- health IDs cannot be cloned, counterfeited or replayed
- Medical Identity Theft is greatly reduced.

[3] See www.lockstep.com.au/press/new-inventors-pod-cast.

References

[1]. Wilson, S. G. *A novel application of PKI smartcards to anonymise Health Identifiers* AusCERT Asia Pacific Information Technology Security Conference, May 2005; see www.lockstep.com.au/library/ehealth/a_novel_application_of_pki_sm

[2]. ASTM *Standard Guide for Properties of a Universal Healthcare Identifier (UHID)* American Society for Testing and Materials, ATSM E1714-07, 2007.

[3]. World Privacy Forum *Medical Identity Theft: Information Crime that Can Kill You*, 2008 www.worldprivacyforum.org/pdf/wpf_medicalidtheft2006.pdf

[4]. Department of Health and Human Services *HIPAA Security Standards; Final Rule* 45 CFR Parts 160, 162, and 164 www.cms.hhs.gov/SecurityStandard/Downloads/securityfinalrule.pdf

[5]. European Commission Fraud Prevention Expert Group *Report on fraud regarding non cash means of payments in the EU*, 22 April 2008; http://ec.europa.eu/internal_market/payments/docs/fraud/implementation_report_en.pdf.

About the Lockstep Group

Lockstep is a privately owned cyber security firm established in 2004 to undertake innovative research and development addressing privacy, identity theft, spam and online social networking safety. In 2007 Lockstep Technologies was awarded an AusIndustry Commercialising Emerging Technologies (COMET) grant with which we developed and proved *Stepwise* applications for health record de-identification, anonymous proof-of-age, and Internet payments security. Lockstep Consulting clients in the health & welfare sector have included South Australia Health, the National eHealth Transition Authority (NEHTA), Commonwealth Department of Health, Medicare Australia, the Australian GP Network, Ozdocsonline, the Australian Privacy Commissioner, and the Victorian Department of Justice.

www.lockstep.com.au/technologies

www.lockstep.com.au/library/ehealth.