Multi-Factor Authentication using Contents from Disparate EHRs
Christopher A. Cassa, MEng1, Kenneth D. Mandl, MD, MPH1
1Chldrn’s Hosp. Inform. Pr og. @ Harvard-MIT Div. of Hlth. Sci. & Tech., Cambridge, MA

Abstract
The development of integrated systems to provide patient-centric health records requires granting access to medical records that have been created at a set of disparate institutions. As many of these institutions no longer have an operational relationship with the patient, this poses a complex authentication problem. We propose a multi-factor authentication framework that allows a trusted intermediate authority to use the contents of potentially matching medical records to generate secondary authentication questions and to manage authorization of appropriate access. This helps to disambiguate between similar records from different patients, as well as ensure that the patient is who she purports to be.

Introduction
There are several methods to directly authenticate a user to a medical document. One is the use a shared secret key such as a previously assigned or agreed password, PIN or biometric hash. This could be created and recorded by the user at point of care or via provider portal. Another method might provide a patient ticket that links her to a records (or location containing subsequent records.) Such a ticket could be provided at a clinical visit, or afterward via email. These methods rely on previously authenticating users (either in person or through email).

Oftentimes, a user may not be able to authenticate in person or electronically. To create a complete health record, it is desirable to integrate clinical data from all institutional relationships, including those that are terminated, or no longer in physical proximity. Additionally, the time and effort required to link to disparate data feeds for patients may not be reasonable, as it is dependent on the number and types of points of care. A suitable alternative that removes the direct authentication burden from patients and providers would solve this issue.

Secondary authentication questions could solve this problem well, though they bring new requirements. One is standardized, structured data so that useful polling information can be gathered. The information value of answering such questions also requires knowledge of the probability of candidate choice events, for example, a visit to a clinic for respiratory infection may be very common, so if a patient selects that choice, it is not very ‘informative’.

Multi-factor authentication framework
We propose a multi-factor authentication process similar to those now required in finance1 to authenticate users with two distinct layers (Figure 1). First, a user accesses her health record portal, and provides identifiers and demographic data. The portal makes a request on her behalf to access health records from disparate institutions by polling a record locator service with her SSN or MRN. The record locator service then polls all participating hospitals to gather a set of candidate records (through a trusted, secure relationship). The record locator service then generates secondary authentication questions which are presented to the user by the record portal. The patient provides answers through the portal, which are transmitted to the record locator service. If the answers are correct, the record locator service will authorize access to a set of records.

![Figure 1. A proposed mutli-factor authentication framework for the retrieval of patient medical records from a set of disparate points of care.](image-url)

Conclusion
A multi-factor authentication process could help solve the complex process of authorizing a user to a set of correct records from all previous points of care.

References
1. Authentication in an Internet Banking Environment.
   http://www.ffiec.gov/pdf/authentication_guidanc e.pdf

AMIA 2007 Symposium Proceedings Page - 891