# Electronic Medical Records – Why Authentication is Critical

Federal government policy makers are looking carefully at the best ways to improve the efficiency of information systems in the healthcare industry. Developing electronic health records (EHR) for all US citizens will require collaboration and coordination of not only the health care providers and the insurance industry but, also the privacy and technology communities. The current approach focuses on exchanging patients' electronic medical records over the Internet at the regional and state level via Health Information Exchanges (HIEs) and Regional Health Information Organizations (RHIOs), then connecting the nation's HIEs and RHIOs to form the National Health Information Network (NHIN)

Our primary concern is how individuals will be allowed access to electronic health records. Thus far authentication and access has received little attention by policy makers, standards and certification organizations. Overlooking authentication of individuals to any health record systems is akin to not installing a lock on the front door to your home.

Health IT is a significant undertaking and authentication of identity is a vital element.

1. Healthcare identity theft and fraud are also significant and growing problems; three percent of profits ($60 billion in 2007) was lost to outright fraud (estimated by The National Health Care Anti-Fraud Association).
2. A recent report sponsored by the U.S. Department of Health and Human Services, "Medical Identity Theft Report," stated that little is done to authenticate the identity of individuals throughout healthcare and concluded that medical identity theft is a significant problem and that consumers have the most to lose. Additional HHS studies by Rand Corporation and Booz Allen support this.
3. At this time the use of two-factor authentication for HIEs and RHIOs to access Medicaid data is currently being debated in the State of New York. NY's Dept. of Health (DOH) contracted Brookhaven National Labs (BNL) as a security consultant and BNL advised the DOH not to grant access to Medicaid data unless each user of the state's (RHIOs) used (two-factor or three-factor) strong authentication via a smart card or hardware token.
4. FY2008 Federal Budget included $1.3 billion in healthcare fraud prevention programs and initiatives. This amount does not include the dollar value of the fraud itself.

While the Health IT provisions in the Recovery Act go to great lengths to detail what is required in the unfortunate event of a data breech, there is almost no language addressing how data breech can be prevented from happening in the first place. Requiring strong authentication as a fundamental principle of any EHR system will ensure those who access medical records are

those who are authorized. Strong authentication will further provide a process by which an audit trail can be established. Such a system would enable:

1. Verification of health care professionals
2. Verification of patients
3. Processes for gaining access to electronic medical records
4. Eliminate fraudulent claims

Protecting an individual's medical information and their privacy is the most important and fundamental element of an electronic health record system. If those protections are omitted then the entire system is undermined. Personal health information is highly sensitive information and warrants the need for very high confidence in the accuracy of the asserted identity of those who attempt to access it. Once it is compromised and into the wrong hands the data contained in it is irreversible and the consequences can affect the victim for his or her lifetime. An NPR poll released the week of April 20 indicated that 76% of respondents had positive impressions of EHRs, however 72% believe their privacy would be violated through EHRs. The security of personal health information is far different compared to other types of personal information including financial. Unlike financial information, there are no policies and procedures in place to restore one's health information once it is compromised. Additionally, organizations and professionals have a fiduciary obligation to ensure transmission of information is properly authenticated between respective parties.

Only Level 4 assurance (two or three factor authentication) as defined by National Institute of Standards and Technology (NIST) provides the highest practical assurance of remote network authentication. Level 4 authentication requires that the claimant prove through a secure authentication protocol that the claimant controls the token. Moreover, the HIEs and RHIOs will undoubtedly be targets of hackers given the nature of the information and those whose private and personal health information is contained. Level 4 authentication prevents eavesdropper, replay, online guessing, verifier impersonation, and man-in-the-middle attacks. **Brookhaven National Labs states on its website that passwords are the single weakest point in the standard site-security model. The majority of security attacks are achieved through password access.**
User authentication that relies on passwords alone fails to provide adequate protection for network systems. Implementation of level 4 assurance by organizations in the US has resulted in a 50% reduction of such attacks.

Similar implementations using such frameworks are widely utilized around the world by developed and developing countries for health care. For well over a decade these nations have experienced lower per capita expenditures on health care than the U.S.

The Health Information Security and Privacy Collaboration's (HISPC) Adoption of Standard Policies Collaborative (ASPC) report to HHS' ONCHIT will establish the minimum requirements for authenticating users accessing electronic health records. Those minimum requirements are not two-factor or three-factor authentication via a smart card, an encrypted token or one-time password device, but rather Level 2 assurance via a "strong" password. The Secure ID Coalition has concerns that stronger authentication methods are not being adopted that would assure the privacy and confidentiality of medical records by having a higher level of assurance that the person accessing the information is who they claim to be and they have a genuine need to view and access the record. It is clear that HISPC is willing to sacrifice security in order to expedite the exchange of health information.

The Secure ID Coalition is concerned that HIEs will be architected only to meet the minimum standards of medium assurance rather than implementing strong authentication to have a very high level of assurance that the person accessing our health information is who they claim to be and have a genuine need to access the information. Any identity system requires strong authentication for the protection of personal information, especially when it is as sensitive as medical information, and consumer privacy.

**We encourage policy makers to ensure our citizens personal health information is protected by mandating at a minimum two-factor authentication into any network containing electronic health records for the protection of consumer privacy.**