Biometrics Answer the Healthcare Identity Theft Problem

The Center for Medicare and Medicaid Services (CMS) is currently in the process of mailing out new Medicare cards to seniors across the nation. Among other changes, the new cards include distinct 11-digit ID numbers, rather than relying upon the 9-digit Social Security Number (SSN).

In the long run, this may reduce the danger that beneficiaries will have their SSN compromised, although in the short term the transition to new cards is creating opportunities for scammers. Moreover, the new cards will do little, if anything, to address the broader issue of healthcare identity theft.

As underscored by recent examples – a home health aide in Connecticut, a hospital employee in West Virginia and another in Oklahoma – insider threats are one of the most common sources of healthcare identity theft. As Protenus noted in its 2017 Breach Barometer Annual Report, insider incidents accounted for the largest share of the 5.5 million healthcare records breached in 2017. Insider attacks are also more difficult to detect and more expensive to combat, especially as increasing amounts of data are being stored in electronic health record (EHR) databases.

All told, according to Healthcare IT News, "The fiscal impact of medical identity theft is considerable, generating losses to the health industry of more than $30 billion each year" citing data from the Ponemon Institute. Patients themselves "also sustain financial consequences of fraud, having to pay an average of $13,500 to resolve these issues." In addition to the time and expense of clearing their names, patients are also in danger of misdiagnosis or even arrest if an identity thief's information gets mixed up with their own.

As many experts have recognized, biometrics provide a solution because they verify that patients are who they claim to be and unmask imposters. A 2012 report from the Healthcare Information Management and Systems Society (HIMSS) highlighted biometrics as a core component of multifactor authentication (MFA), explicitly listing fingerprints and voice recognition as biometric modes which can easily be integrated into a Health Information Exchange (HIE). In 2016, Grand View Research also identified iris recognition, palm vein recognition, and DNA as viable candidates for biometric authentication in a healthcare context.

What seems certain is that, regardless of band-aid fixes like new Medicare cards, healthcare identity theft and fraud will continue unabated until America's healthcare system adopts a protocol, which uses smart cards and biometrics, for identifying patients and securing their healthcare data.