Banking on PUBLIC TRUST

In the future, more people are likely to begin accessing their medical information using banking platforms. The movement toward higher deductibles, greater patient responsibility for payments and price transparency is leading to specialization of banking platforms in order to manage investments in account-based health plans, such as health savings and reimbursement accounts (HSAs and HRAs). This new health-wealth paradigm is steering market leaders to integrate health data oriented tools with financial services. As this occurs, some are asking if commercial banks are addressing issues of public trust in this emerging area.

It is important to note that the market is asking this question not just of banks, but of all types of health information exchanges (HIEs). Equally important is how this question applies to the business-to-business realm as banks develop health data services that fundamentally streamline transaction costs. In late 2007, a group of commercial firms, providers and health plans formed HiTRUST to implement a security framework for HIE. The group intends to unveil a framework after a 12-month gestation period. Other groups are weighing in too. For example, the Markle Foundation announced at a high level session in 2007 that it too was working on a privacy framework for HIE.

These activities fall on the heels of legislative and private efforts to create a common framework for security and privacy in the emerging panacea of digitized, on-demand health information. For example, the CMS Office of the National Coordinator (ONC) has been working on a privacy framework that it hopes to publish in 2008. Another effort, based on the health record bank model, met in 2007 to draft legislation favorable to the creation of such banks in addition to establishing that HIPAA-defined privacy and security protections must be implemented by new health record trusts. The Independent Health Record Bank Act of 2007 did not gain the anticipated traction and the group working with privacy factions is now vetting a new version of the rule that mandates a privacy and security framework. Moreover, privacy groups affiliated with the effort insist that HIPAA is inadequate. They want more restrictions, such as mandating patient consent prior to disclosing health information. HIPAA permits use of patient information without consent for "treatment, payment and operations" in order to not slow down or complicate the processing of payments or delivery of care. Privacy groups assert that this is tantamount to a gaping security hole that lets health data be used inappropriately.

Groups like Microsoft's HealthVault and Google Health's newly announced program would be affected by this act, as well as other groups forming health record banks or electronic record hosting services, such as Kentucky's LouHIE or Rhode Island's HIE effort. Clearly, groups working commercially or as part of a government effort will be increasingly tested by the marketplace as they evolve to ensure that they have a fail-safe approach. Some fear that digitizing health data will lead to increased privacy risks for everyday consumers. Others disagree, noting that tightening up existing laws will add cost and complexity without the corresponding benefits. Is the fear of loss of privacy in the digital age a legitimate concern? After all, consumers are being urged to create and store digital copies and few would disagree that this could become a digital recipe for disaster without the right controls.

Unfortunately, we do not need to look too far to see a case study. The recent revelation that the IT and customs department of Britain lost personal information of almost 50 percent of its residents – data that could be used to heist identities – is considered the world's biggest security disaster in the computer age. This did not make it any easier for the UK healthcare authority to convince doctors to ramp onto their national health information exchange. The U.S. model for HIE is different in that multiple HIEs and/or PHR banks would link to each other as opposed to having one big database. Yet the challenges and risks remain the same. In the UK, a number of doctors have revolted, leading to considerable angst about where to take the program next.

AN INDUSTRY PILOT

As early as 2001, the Medical Banking Project (MBProject) called on industry leaders to implement a new type of accreditation program that utilized privacy and security frameworks outlined in healthcare and

By **JOHN CASILLAS**,
Founder, Medical Banking Project

banking laws. After driving HIPAA into the banking arena – which the project felt was a prerequisite to create a new medical banking industry in which banks could specialize their services for healthcare – a whitepaper was drafted, examining regulatory requirements for banks offering health data services. In it, the project defined a new bank-based, health data clearinghouse that it believed could emerge in the post-HIPAA environment.

This type of banking program, the project reasoned, was tied to the inter-organizational systems (IOS) theory developed in the 1990s. IOS theory holds that when two adjacent industries mature in their use of electronic data interchange, they tend to link processes to reduce redundancies (i.e., retyping data from one system to another). This occurred in the airline industry when Sabre changed the competitive paradigm by integrating ticketing systems with financial networks. The result is that today people can go online to make reservations without calling travel agents. Developing the medical banking theory, the project asserted that as HIPAA drove digital processing in healthcare, linkage between banking and healthcare systems would revolutionize costs for administrative processes.

No longer theory, medical banking appears in full swing as multiple banking and healthcare firms announce new hybrid programs. For example, in 2003 PNC Bank announced that it was creating a new healthcare program and later acquired a health data clearinghouse. The SSI Group, a health data clearinghouse, and Bank of New York Mellon announced an alliance to implement new medical banking programs; McKesson, one of the world's largest hospital information systems vendors, announced a strategic alliance with a major bank; BancTec, a banking IT solutions vendor, announced a new medical banking service, to name a few. New banking investments in treasury management have proven that the theory behind medical banking and deeper systems convergence is inevitable. Today, think tanks like Gartner, Booz Allen Hamilton and McKinsey recommend and confirm this growing trend.

As markets tilted toward medical banking, MBProject urged leaders to assess the impact of data privacy regulations like Title V of Gramm-Leach-Bliley, FACTA and PCI within the credit card industry, HIPAA's privacy and security

regulations, FFIEC guidance on authentication in the online banking environment and others. A workgroup was formed within the Project in 2007 – the Accreditation Review Council – to develop a matrix of regulations, accreditation programs and to talk through the issues. This process took 15 months and led to the creation of the Gold Seal accreditation program for medical banking constituencies.

INITIAL GOALS OF THE PILOT PROGRAM

The mission of the Gold Seal program is to instill public trust in medical banking programs. The workgroup was guided by the following principles:

- To isolate all of the rules and regulations in the healthcare and banking/financial services industry that impact access and use of consumer and/or customer health data
- To create a matrix of the rules and all related accreditation programs in the healthcare and financial industry domains
- To perform a gap analysis of the rules and accreditation programs, noting areas of redundancy that add cost to compliance auditing and to develop a new accreditation program or implement another approach if necessary

Equipped with this data, the group was determined to develop an appropriate strategy to support its mission. To manage the accreditation criteria, a series of privacy and security protocols were reviewed by the workgroup that were part of an online tool designed by Milliman, a global actuary firm that conducts HIPAA audits for health plans, third party administrators and others. Prior to the implementation of the pilot, MBProject conducted a survey at its annual membership forum to ascertain the attitudes of medical banking leaders toward a Gold Seal program. Seventy percent felt accreditation was "somewhat important" to their organizations and of these, 50 percent said they would implement a Gold Seal program in seven to 12 months if it became available.

Buoyed by this confirmation, MBProject contracted with Milliman to administer a two-day pilot program at the Working Capital Solutions division of The Bank of New York Mellon (BNY Mellon). The three organizations entered a non-disclosure agreement. BNY Mellon set a target date that was moved a few times in order to gather all of the necessary subject matter experts (SMEs) that were needed – 23 in various departmental areas – after which a post-pilot survey gauged reaction from those tasked within the program.

EXECUTIVE FEEDBACK

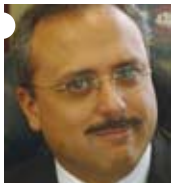
The program was well-received by the pilot participants at BNY Mellon. Several felt that the program may be used to improve and further automate internal processes. With the right SMEs, many of the modules could be completed within a day, thus having the right SMEs identified upfront is critical to an efficient auditing process using the Gold Seal program. Importantly, the project wanted to implement a program that focuses on the needs of financial institutions serving healthcare organizations. The current accreditation programs tend to be very focused on healthcare and not financial services. The Gold Seal program addresses this issue.

The participants also found room for improvements. An example of this is the current use by many banks of the SAS 70 audit, a program intended for auditor to auditor communication that has become a de facto standard for good information practices (note that according to PricewaterhouseCoopers, the SysTrust™ audit is more appropriate for IT auditing). In creating the Gold Seal program, the workgroup hoped to reference the SAS 70 in order to preclude the obligation to reassess similar operational areas with identical criteria. The pilot program proved otherwise, however, in that accounting firms that do SAS 70 typically impose restrictions on how results can be referenced. Thus, areas that could have been accredited without an on-site visit, for example, may need to be reassessed in the Gold Seal program. There were many other helpful comments from the pilot participants that will serve to improve the program.

With the pilot completed, the workgroup is now preparing a presentation and a formal recommendation to the industry for adoption of the Gold Seal program at the Sixth National Medical Banking Institute in Marietta, GA from April 1 to 3, 2008. Protocols will be posted on the project's public Web site so that other groups can assess and critique the privacy and security framework used within the program. The workgroup intends to continuously review protocols to ensure that they are responsive to new laws, policies and frameworks developed by ONC, commercial groups and those policies sanctioned by the National Governors Association, specifically in its role administering the State Alliance for e-health initiative that captures best practices for evolving HIEs.

CONCLUSION

Since MBProject's recommendation in 2001 to implement a privacy framework for medical banking constituencies, the industry has flourished. This emphasizes a growing need to meet this critical recommendation. Establishing HIPAA's impact on banks was a vital first step toward creating a framework of public trust. Yet HIPAA is one of several laws that a Gold Seal program must implement. Reducing transaction costs, the push toward medical consumerism and the globalization of healthcare is thrusting banks into the center of a paradigm shift in healthcare. As this occurs, it is critical that medical banking constituencies form a vanguard against reputational risks by implementing a Gold Seal program. A solid program will demonstrate to government and industry that public trust is a bedrock of new banking programs that improve healthcare. **FH**



JOHN CASILLAS founded the Medical Banking Project to facilitate the integration of banking and healthcare systems. John created a series of industry-recognized forums that shaped the national debate on the impact of HIPAA on banks, launched a national lecture series dubbed, "The Great American Interoperability Tour" to create awareness about the role of banks in transforming healthcare and founded the Medical Banking Institute. He is recipient of the 2005 and 2006 Healthcare 100 Award. He was HFMA's medical banking SME from 2001-2004.

EMDEON

AD