

Testimony
by
John Casillas
Chief Executive Officer of BoardTrust, LLC.
to the
National Committee on Vital and Health Statistics
Subcommittee on Standards

Hearing titled:
Section 1179 of the Health Insurance Portability and Accountability Act

May 6, 2015

Thank you for inviting me to participate in this hearing. I represent BoardTrust, LLC., which provides strategic advisory to the private and public sectors by helping them to engage global health using medical banking principles. The integration of mobile banking/finance and mHealth to reduce costs and increase access to healthcare among the poor is one example of this area. Another is the integration of banking and healthcare administrative systems, such as the bank lockbox and patient accounting platform for moving the “paper chase” in healthcare onto a digital processing platform. This area has now been implemented by all major US banks. Point of service transaction processing is a very active area today in medical banking. There are also initiatives where banks are deploying expertise and persistent investments in authentication (identity access and management mechanisms) to provide consumers with trusted access to their health records.

Beginning in 2001, The Medical Banking Project (an effort I started that was acquired in 2009 by HIMSS, a global health IT cause-based organization) engaged the public and private sector and academia in a number of venues – roundtables, institutes, leadership forums – to isolate policy issues around the topic of HIPAA’s impact on banks and financial institutions. At the time significant policy issues surfaced in the marketplace that were rooted in various interpretations of Section 1179. I sought to clarify these issues by inviting the government, commerce and academia to dialogue impact. By 2004, we were able to steer this dynamic to support much needed innovation in healthcare, which was and remains my top priority. Our work was documented in white papers and a HIPAA compliance section of “A Medical Banking Road Map for America”, Version 1 and 2; segments of which have been included in my testimony.

I believe today’s dialogue is long overdue, especially within the context of how far the marketplace has come in implementing medical banking programs since 1996, when I began facilitating the medical banking segment and writing about potential policy impacts of HIPAA’s upcoming Privacy Rule. It was the Privacy Rule that brought the issue of section 1179 into national prominence. It is essential to engage policy issues around what lies in the immediate horizon for improving cost, access and quality of care due to innovations that lie at the nexus of banking, healthcare and technology.

Medical banking principles evolved over a 10 year period. At the time, I became very interested in the potential application of “inter-organizational systems” theory (Konsynski and Cash, 1992) between banks and healthcare providers. I believed that banking and health IT linkages could drive significant innovation. A diverse stakeholder constituency, from banks to health IT firms to auto, pharmaceutical and even entertainment giant Disney, joined “The Medical Banking Project (MBProject)” to evolve this innovation. After MBProject’s unification with HIMSS in 2009, the World Bank also signed on, supporting what one global consultancy called a “medical banking movement” and creating a new fellowship position that I assumed and today remain as fellow emeritus.

Section 1179 of the Health Insurance Portability and Accountability Act (HIPAA) statute was the subject of intense and exhaustive outreach to government, commerce and academia, with HIMSS Medical Banking Project (HMBP) conducting twelve national roundtables over 24 months (2001-2003), 13 national medical banking institutes (2002-2013), and numerous additional forums that collectively coalesced 800+ government officials in banking and healthcare, healthcare providers and large health plans, associations in banking and healthcare, commercial bankers, health IT vendors, policy consultants, university professors and many others.

I often comment that medical banking is a journey. There are many facets around the cross-roads of banking, healthcare and technology. This includes all the respective policy issues in each domain, a range of technologies that are complimentary across domains, credit resources and large investments in infrastructure – all of which is constantly being positioned in a competitive marketplace to yield value. These emerging efficiency platforms have made significant contributions to cost, access and by virtue of impact of these two, quality of healthcare. One healthcare provider is saving \$4 million annually using a medical banking platform, for example. Also of note, the benefits actually fall disproportionately to smaller hospitals and providers who can use operational savings to support community missions around charity care. This theory was confirmed by an independent survey sponsored by a large bank, affirming MBProject’s thesis and mission (from 2001 to 2009) to “convert digital savings into charitable resources”.

Among the innovations and developments that lie at this nexus is of course, the application of section 1179 of HIPAA in the marketplace. In my reading of the legislative history of this section, there appears substantive consideration of how HIPAA should apply to banks. Nevertheless when my findings were published in a privacy newsletter in 2001, it set off a storm of debate that persists today. While the topic is complex, I want to synthesize our work over the years into three distinct points of policy and/or principles. I know that this is just the beginning of understanding how to evolve policy in this cross-industry domain; we are talking about the nexus of two highly regulated industries who view health data from their own perspectives. Each has a strong and vested interest in ensuring strong protection of health data that enters their respective domains. It is my belief that if we can collectively come to an understanding

around these three areas, that it will lay the groundwork for informed action around other cross-industry policy issues that will likely need to be addressed as medical banking programs are adopted.

1. **Although the OCC lists traditional health data clearinghouse services as a permissible national bank activity that is incidental to the exchange of payments in healthcare, only electronic funds transfers (EFT) appear to be exempted from HIPAA.**

I would like to discuss OCC's comments around banking engagement in health data but first, I want to point out that the legislative history is clear, as well as a studied reading of Section 1179, that this section of HIPAA¹ was implemented to exempt *consumer-initiated financial transactions*. According to the author of the section,(at a policy forum we organized during a WEDI event), section 1179 "was never intended to exclude banks. Period." Furthermore, the individual who facilitated creation of the language for section 1179 testified in a previous NCVHS hearing that this section was developed at the request of the credit card sector who wanted to exchange funds without the impediment of HIPAA compliancy.² This is important because it speaks towards intent and ultimately function; specifically, the function or role that banks and/or financial institutions play in transferring money.

A strict reading of section 1179 reveals that all the functions enumerated apply to money or funds transfers and not to remittance data. For example, remittance data is never cleared, settled or billed. Furthermore, remittance data is comprised of HIPAA-defined protected health information that is covered under the HIPAA statute.

While is likely much of the information around this area has been covered by this Committee, I want to go back just a bit to include the language of HIPAA and related commentary. The statute defines individually identifiable health information as:

"...any information, including demographic information collected from an individual, that-- (A) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and-- (i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual."³

¹ William R. Braithewaite worked at HHS during the formative period of HIPAA and was responsible for, among other things, assessing policy in the banking and financial services industry.

² Tom Gilligan was a senior lobbyist who worked with certain credit card firms, and HHS, to craft appropriate language that enabled use of credit cards for funds transfers without the potential impediment of HIPAA; that eventually came to be known as section 1179.

³ *ibid*

Within the context of payment, HHS draws a clear line between the transfer of funds data (i.e., amount, routing number, etc), and a transfer of remittance data (i.e., the explanation of benefits that often contains medical codes and procedure descriptions). Note the HHS commentary:

“...a covered entity may conduct the electronic funds transfer portion of the two payment standard transactions [820 and 835] without restriction, because it contains no protected health information. The protected health information contained in the electronic remittance advice or the premium payment enrollee data portions of the transactions is not necessary either to conduct the funds transfer or to forward the transactions. Therefore, a covered entity may not disclose the protected health information to a financial institution for these purposes.”⁴

HHS clarifies this policy as follows:

“The transmission of both parts of the standards are payment activities under this rule, and permitted subject to certain restrictions. Because a financial institution does not require the remittance advice or premium data parts to conduct funds transfers, disclosure of those parts by a covered entity to it (absent a business association arrangement to conduct other activities) would be a violation of this rule.”⁵

We found that upon examining all of the information, the section 1179 exemption extends, and ends, at *funds transfers* between health plans and providers and between consumers and providers. Beyond transferring funds, if the bank is processing remittance or eligibility data, for example, in the form of paper “explanations of benefit” (EOBs) or electronic remittance advices (ERAs), this would not be an exempted activity.

While this seems clear, we believe NCVHS should consider policy positions of the Office of the Comptroller of the Currency (OCC). OCC maintains a list of “permissible activities” for national banks. In other words, banks that perform these activities are complying with federal guidance. To further expand on this, I pulled a section of a position paper I wrote in 2006 outlining business models and compliance issues for “bank-driven electronic health records” as follows:

“The OCC acknowledges that the “business of banking is an evolving concept and the permissible activities of national banks similarly evolve over time.”⁶ While the OCC seeks to limit that activities of “National Banks” to “activities that are part of, or incidental to, the business of banking”⁷ they also note that other activities may become authorized for a national bank.

The OCC then sets out a non-exclusive list of permitted activities, noting that “any activity described in this summary as permissible for a national bank is also permissible for an operating subsidiary of a national bank. The reverse is also true: any activity described as permissible for an operating subsidiary is also permissible for the bank to engage in directly.”⁸

The OCC provided a conditional approval to Nation’s Bank in 1996 regarding plans to acquire a health data clearinghouse. In the Approval, an OCC regulator comments:

⁴ 65 *Federal Register* 82462, 82496.

⁵ 65 *Federal Register* 82462,82616.

⁶ Office of the Comptroller of the Currency, *Activities Permissible for a National Bank*, 2005, p 1.

⁷ *Ibid*

⁸ *Ibid*

As long as ten years ago, the OCC approved national bank participation in a limited partnership whose activities were very similar to those of EHS. Interpretive Letter No. 419, reprinted in [1988-1989] Transfer Binder Fed. Banking L. Rep. (CCH) ¶ 85-643 (February 16, 1988). The purpose of the limited partnership in that case was to “develop a data processing system linking health care providers, health care insurers, health care recipients, and their respective depository institutions.” The system, known as EXCLAIM, would “transmit claims eligibility information, receive and transmit information for claims entry and payment, [and] operate a data base.” A notable feature of this system was that it included the transmission of treatment information by health care providers to health insurance carriers, used by the carriers in processing the insurance claims, a feature that will also be included in the EHS system. In fact, the activities of EXCLAIM went beyond those in which EHS proposes to engage, since they included the development and licensing of software necessary for clients to participate in the system. EHS, as noted above, intends only to acquire software from unrelated vendors.⁹

In a footnote, the OCC shows precedence for electronic healthcare services as follows:

There are many other OCC precedents relating to health care or health insurance support services. See, e.g., Corp. Dec. No. 98-13 (Feb. 9, 1998) (operating subsidiary whose activities included providing medical insurance cost information and benefits counseling); Interpretive Letter No. 712 reprinted in [1995-1996 Transfer Binder] Fed. Banking L. Rep. (CCH) ¶ 81-027 (Feb. 29, 1996) (factoring of medical receivables, including filing of related insurance claims); unpublished letter of Horace Sneed, Senior Attorney (Dec. 6, 1993) (completing and submitting insurance claims on behalf of medical care providers). In addition, the Federal Reserve Board has found the operation of a medical payments network, including the processing and transmission of medical and coverage data, to be a permissible activity for bank holding companies. Banc One Corporation, 80 Fed. Res. Bull. 139 (1994). Bank holding companies, of course, are governed by a different statute than national banks. Nevertheless, the standards of “incidental to the business of banking” under 12 U.S.C. § 24(Seventh) and “so closely related to banking or managing or controlling banks as to be a proper incident thereto” under section 4(c)(8) of the Bank Holding Company Act are very similar.¹⁰

OCC provided the following Conditional Approval to a national bank that was seeking clarification regarding whether processing health information is a permissible banking activity:

“The OCC has long recognized that the transmission and handling of medical and health insurance data in connection with activities such as funds transfers, billing services, or claims processing, is an activity that is incidental [to] the business of banking.” [brackets supplied]

In another Conditional Approval, the OCC again outlines its views:

The OCC has determined that a wide range of insurance-related administrative services are authorized for a national bank or its operating subsidiary. It is well established that national banks may provide billing, collection and claims-processing services as an activity incidental to the express authority to engage in processing payment instruments. See Interpretive Letter No. 712, reprinted in [1988-1989 Transfer Binder] Fed. Banking L. Rep. (CCH) 81-027(February 29, 1996); Interpretive Letter No. 718, reprinted in [1988-1989 Transfer Binder] Fed. Banking L. Rep. (CCH) 81-033 (March 14, 1996). Billing, collection and claims-processing services may include collecting and processing insurance premiums and processing insurance claims. See Corporate Decision No. 98-13, supra. Handling medical and insurance data in connection with these activities is also authorized. See Conditional Approval No. 282 (July 31, 1998).

⁹ Conditional Approval #282; August 1998; Letter from OCC to Nation's Bank.

¹⁰ *Ibid*

The OCC is clear about what banks can engage in. In my opinion, the Department of Health and Human Services should be equally clear in asserting its role for overseeing medical banking market structures.

The OCC, I believe, accurately predicts that the “business of banking is an evolving concept and the permissible activities of national banks similarly evolve over time.”¹¹ I believe that medical banking clearly fits into this category. A policy issue therefore may be that as banks evolve their business lines, does this automatically exclude or exempt them from the existing policy regulations that govern those lines of business? If we are to conclude that section 1179 fully exempts banks, does that also mean that health data privacy is left to banking policy constructs irrespective of the constructs that have been developed in healthcare? Do those policy constructs come under the informed positions that resulted in some 50,000 comments that HHS received on the HIPAA Privacy Rule alone, for example?

I ask these questions not to be combative, or to suggest that section 1179 should apply to banks because of this line of reasoning. We have found many other reasons for applying the section to banks. I simply believe these are sound policy questions as NCVHS engages the topic of section 1179.

Recommendation: HHS should implement a cross-stakeholder panel of independent experts that can meet on a regular basis to review evolving medical banking policy issues. Given the significant and persistent investment by banks into the health IT domain, and the forward focus of electronic healthcare to engage consumers that I believe invariably involves banks and financial institutions via integration of online banking and mobile payments/finance with mHealth, debates will continue to surface around “policy friction” between these two large industries.

2. Symmetrical application of HIPAA across all market structures.

At a roundtable organized by HMBP at the 3rd National HIPAA Summit, industry experts, including a senior policy advisor at HHS/OCR, discussed the application of HIPAA to banks. The advisor was very clear: *no sector was omitted from HIPAA*. We reviewed this issue numerous times starting in 2001, when the Bush Administration let the Privacy Rule stand as is. The HIPAA legal construct establishes that any entity that uses, discloses or has access to PHI from a covered entity must be governed by a business associate contract. HITECH took this a step further, implementing the same potential penalties for a business associate as are placed upon a covered entity.

Clearly, however, this remains a “burning” policy issue. If some groups use and/or access HIPAA-defined PHI, but are not federally mandated to comply with HIPAA, and other groups have similar use and/or access to PHI but must comply, there would appear to be a fundamental misalignment between actors in

¹¹ Office of the Comptroller of the Currency, Activities Permissible for a National Bank, 2005, p 1.

the same ecosystem that I believe will tend to increase administrative costs. Our work showed how integration of banking and health administrative IT systems can significantly reduce administrative costs – moving the “paper chase” in the business of healthcare to a digital platform. The same dynamic occurred in the airline industry when the banking system was integrated into the airline reservation system (the SABRE system), displacing intermediaries and driving administrative costs down. In fact, the reason why we can go online to do our travel today is because of this platform innovation. I envision the same evolution for healthcare in the near future where health payments can be managed, records can be pulled and where telehealth/telemedicine programs can thrive. We already see the convergence of banking and health IT in many ways throughout the marketplace.

It is important to note that there are now, by virtue of the business models evolved by the community at HMBP, *bank-owned health data clearinghouses*. Even prior to my work in this area, there were banks that were performing HIPAA-defined clearinghouse services, a fact that was independently corroborated by a taskforce organized by banking organizations after our roundtable discussion at the 3rd National HIPAA Summit. Their report noted, and NCVHS indicated assent in its letter to HHS in 2004 advising same, that while the vast majority of banks aren't a HIPAA-defined clearinghouse there are some who are. Notably, those that fit this description are typically the nation's largest banks with global reach.

From a policy perspective do we allow for two “clouds” – one that must comply with HIPAA and the other that doesn't? Its a significant policy issue because HIPAA's Privacy Rule was implemented for the very purpose of protecting an individual's private health data in a very particular way that you don't necessarily see in Gramm-Leach-Bliley, FACTA or PCI – each of which are quite sound, but they have different perspectives. If we engage in the asymmetrical application of HIPAA policy across market structures, we may find a heterogeneous policy environment of bank-owned health data systems, where HIPAA compliance is irrelevant, and non-banked owned health data systems where HIPAA applies. More of the traditional “health data clearinghouses” may find it advantageous, from a competitive standpoint, to merge with a bank (some already have) to avoid HIPAA and its associated costs altogether.

From a business development perspective, remember that as the industry moves from paper to electronic transactions in the business of healthcare, a digital ecosystem is emerging to move data as efficiently as possible. Here is where banks have a dominate presence via persistent investment and innovation. Net margins are relentlessly driven by administrative excellence in the banking domain. Fortunately for all of us, hospitals and physicians drive towards clinical excellence and so it stands to reason as the ecosystem moves from paper to electronic, administrative practices honed and sharpened by banks will rise in importance in healthcare. The banks are the ones moving the \$2.5 trillion in our national healthcare expenditure. Movement of funds, and remittance data, is essential to the sustainability of the healthcare

enterprise. Many healthcare providers have focused investments on remittance management IT and work with their health data clearinghouses and banks to ensure efficient operations of this critical function.

As the business of healthcare goes digital, and clearly the OCC conditional approvals cited earlier appear portentous of this direction, banks may continue to move into the health domain to create more efficient “payment” systems (claims operations, eligibility via card swipes, authorizations for health benefits, payments, healthcare remittance advises, etc). I think this is extremely exciting and ripe with potential for improving health business systems, yet, as this dynamic comes into being it is vital to sort out the policy issues related to use, access and disclosure of PHI.

Recommendation: Educational materials are needed for the banking community. Many in healthcare are already sensitized to the issues around health data privacy but I believe that banks have not had the same type of education relative to HIPAA. While our venues sought to do this, our funding came initially from my “back pocket” and then later from some 65 corporate members...but it was not nearly enough to meet the need. Industry groups like HIMSS, NACHA, WEDI, EHNAC (that evolved a bank HIPAA compliancy program that stemmed from a recommendation from The Medical Banking Project), and others, are vital for this effort. Please note that these groups have already collaborated on creating a policy document enumerating actions that should be taken to implement a HIPAA compliant operating environment that could become a basis for education.¹²

3. Healthcare payment innovation and new forms of healthcare credit, especially as we move towards e/mHealth, will evolve cross-industry policy issues in banking and healthcare.

What if you could swipe a card and initiate all the transactions (HIPAA’s Transaction & Code Sets Rule specifies multiple administrative transactions) related to a patient visit? There are companies that are working on this “holy grail” for health payments. Its actually quite a technical process to know in an instant if the person holding the card is truly who they say they are (a distinct transaction), know their current benefit level (another transaction), know their current benefits and to what extent they are reimbursable (another transaction layer), to initiate an accurate payment (transaction(s)) and then to receive remittance data (final transaction) that can automatically be posted into the patient accounting system and furthermore, kick off downstream workflows as well as fuel business intelligence for managing the practice or enterprise. A “payment” in healthcare, of course, isn’t like a payment in the grocery store. On the other hand its complex with multiple data inputs, many of which contain PHI.

Notably some firms have already implemented a subset of the transactions described above at point of service, linking health data and banking systems to achieve lower administrative costs and greatly

¹² <https://healthcare.nacha.org/sites/healthcare.nacha.org/files/files/FI%20Compliance%20Guidelines-08102012%20Update.pdf>

simplifying the complexity of paying healthcare bills while improving consumer/patient satisfaction. Also important to note: the technological configuration may or may not permit bank's use, disclosure or storage of HIPAA-defined protected health information. A bank that is part of a value chain may have zero access to PHI. Others, however, may contain a subset of data protected under HIPAA.

To this point, we asserted earlier that section 1179 carves out "consumer-initiated financial transactions" so how do you reconcile this exemption with the current trend towards robust transaction management at point of service? We believe you can do this with full policy integrity by using the discussion in point 1: if funds are being transferred, the activity is exempted but anything other than funds would not come under the exemption.

The issue also touches on a point of policy that we explored related to what organization is responsible for HIPAA compliancy in a value chain. Ultimately, based on commentary from CMS and discussions in our forums, it was determined that the entity named in a contract for services with a covered entity, where PHI is used (in this case for operational purposes), would more likely than not be held to HIPAA compliancy standards regardless if the entity had access to the PHI used for this purpose. Notably, this was our finding based on the facts at that time and others may have different results depending on how the value chain is structured. I bring this up however to demonstrate the range of policy considerations in medical banking and the potential need to continuously clarify policy as market structures emerge.

Given the focus on section 1179, I am somewhat reticent to point out another policy area that stems from HIPAA's impact on healthcare credit practices. These issues are documented in my work but they are tangential to the topic. The issue arises when a bank collateralizes its loan using healthcare receivables. Unlike other "invoices", the healthcare claim and PHI are inextricably bound. So what happens when the provider violates a contractual provision of the loan, forcing turnover of the collateral? There was no pretext initially for a business association; the bank simply provided a loan to the provider. Yet in this circumstance, which is not uncommon, the bank gains access to healthcare receivable and thus PHI external to HIPAA and now must find a mechanism to process the receivable in order to extract its monetary value. This is a complex area that involves the legal concepts of "true or absolute sale" and the individual's new right to private health data that was enacted under HIPAA. If the Committee would like to engage this area I can share a white paper on the topic.

Recommendation: Policy executives should actively engage and speak at educational forums that are at the nexus of banking, healthcare and technology. This is a quickly evolving area, especially as the types of payments have multiplied in the marketplace (moving to mobile domain). In addition, account-based health plans like HSAs, HRAs, etc., (ironically, also evolving from the original HIPAA statute), lead to "multit-purse" capability that enables a consumer to use funds personally or from other accounts to pay for

healthcare. Understanding how this market is evolving is vital from a policy perspective as banks address security and privacy across all the payment mechanisms. In our work at HIMSS Medical Banking Project, it was essential to have HHS at the table so that as these new formats evolved, we could have productive policy discussions and alert policy executives as to future innovations.

In closing, I don't believe that the framers of HIPAA envisioned compliant versus non-compliant "clouds" for health data. They were concerned about how our health information might be used as the industry moves from paper to electronic processes that support the care we receive. They didn't want "Aunt Anna" or an elder caretaker worried about the confidential health information of Mom or Dad. I also believe that they understood somewhat of the complexity of the national undertaking to keep our health information secure and confidential when they implemented HIPAA.

I think a detailed study of Section 1179 will show that it exempts funds transfers in healthcare payments and nothing more than that. When banks engage in activities beyond that, and I sincerely hope that they do because the scale and efficiency that can be leveraged to support our national health goals, they are likely operating in way that should comply with HIPAA.

I've attached additional information to further elucidate positions taken on the issue of Section 1179 and its impact on the banking and financial services industries. Please do note, however, that due to time limitations in learning about this particular session, I was only able to provide the information "as is" without editing specifically for this hearing. The documents cited come from "A Medical Banking Road Map for America" and involve our collective understanding at The Medical Banking Project *at that time*, prior to acquisition by HIMSS. I include them because they do, however, provide information and citations that are relevant for understanding the impact of policy in the medical banking sector, the types of banking services that might be impacted and how they might evolve over time. The full volumes are available on the HIMSS.org website.

Thank you again for the opportunity to provide testimony around this key policy issue.

Sincerely,

John Casillas
Chief Executive Officer
BoardTrust, LLC.

***** Excerpts from “A Medical Banking Road Map for America” published by MBProject *****

From 2001-2004, the Medical Banking Project organized a series of outreach and educational forums to isolate cross-industry policy issues and commercial opportunities that can be developed between financial institutions and the healthcare industry. This resulted in the formation of five broad areas of focus which formed the basis for our workgroups:

1. **Improving operational efficiencies in healthcare administration**
2. **Compliance and public trust**
3. **Improving liquidity in healthcare**
4. **Improving healthcare access**
5. **Identifying potential threats to our national healthcare system**

Each workgroup has evolved separately through collaboration with industry groups, government and others. MBProject aggregated work in an online portal and from this, created an action template for each workgroup. The template was modified in 2004 during online workgroup meetings. From this effort, Working Papers were developed and catalogued in this volume.

We acknowledge this is a very early work. Much more must be done to collect all the requisite information, distill concepts and provide a meaning “medical banking road map for America”. We hope that this effort will provide a meaningful glimpse of how medical banking can substantively improve healthcare for commerce, government, charities and others.

Workgroup Grid, MBProject 2005

Workgroup	Leader/Co-Leader	Focus Area	Previous Work Efforts
Workflow Automation Council	Nav Ranajee, LaSalle Bank (ABN AMRO)	Improving operational efficiencies in healthcare administration	Panel at the 2 nd National Medical Banking Institute with Wachovia, INOVA Healthcare System in DC; HFMA HIPAA@Work Task Force.
HIPAA Compliance	John Casillas, MBProject; Catherine Warren, Bank of America	Compliance and public trust	Numerous published articles, presentations
Healthcare Credit Practices	Leslie Bender, JD, ROI Companies	Improving liquidity in healthcare	Published Articles: The Banking Law Journal (Casillas & Romero, May 2003); Credit & Collections Practice (FN); ACA Journal (FN)
Charity	Tom Dean, CEO, Critical Technologies	Improving healthcare access	Advisor: CCN Pilot programs
Cyberwar	Robert Thompkins-Bey,	Identifying potential threats to our	Panel presentations:

	CEO, Bey Technologies International, Inc.	national healthcare system	Terror & Technology Conference, 2003
--	---	----------------------------	--------------------------------------

HIPAA Compliance in Medical Banking

The banking industry has created an environment of public trust. This is in part due to rigorous and systematic assessment of constantly emerging financial risks, systems that codify best practices into standards and drafting clear regulations governing funds management. Accordingly, today's privacy environment has led to considerable change in banking compliance, regulations and supporting market structures. For example, Title V of Gramm-Leach-Bliley and FACTA have emerged to institute standards around the use of personal healthcare information that comes into the banking system. In a de-regulated environment that permits banks and insurance companies to merge, a privacy issue was accurately forecasted.

While the Administrative Simplification subsection of the Health Insurance Portability and Accountability Act of 1996 or "HIPAA" is largely derived from assessments in the healthcare community, both the original statute (Section 1179) and subsequent regulations (see Privacy Rule commentary relating to banks) have exposed areas of potential privacy and security risk in the services that banks provide for healthcare. The impacted bank service areas include (others may also be impacted):

- Cash management (lockbox, cash disbursement)
- ACH networks
- EDI payments processing (remittance consolidation)
- Lockbox processing
- Healthcare credit practices
- Online/mobile payments
- Credit card operations
- HSA/HRA/MSA/FSA/etc. support
- Data mining

HIPAA has resulted in new banking programs that are specialized for the healthcare sector. These product formats tend to forge new operational linkages between banks and healthcare. Within this context, an increasing number of banks are leveraging substantial investments in technology to support healthcare administrative operations. While it is difficult to calculate the macro-economic "displacement cost" (i.e., the IT costs healthcare could save if by banking engagement), it is safe to say that the impact of HIPAA on banking services for healthcare appears substantial, pervasive and promising. As banks help providers to ramp onto digital networks, the administrative vision of HIPAA to reduce overall costs

seems possible. In addition, new digital networks supported by banks appear to compliment the national drive in America to implement healthcare information networks. Thus the “medical banking” paradigm appears consistent with national policy goals.

Banks routinely invest about three times more in transactional architecture relative to health providers (KPMG, 2001). HIPAA transforms a paper-laden process for managing claims into a digital platform that offers efficiency to the healthcare stakeholders, including banks. Since HIPAA’s Privacy Rule was enacted, banks and financial institutions have leveraged substantive investments in transaction architecture, business process know-how and even credit resources to reduce processing costs in healthcare.

Another dynamic that factors into this new model is the wholesale transformation of bank revenues from interest to fee-based income. This is in economic effect tantamount to the transition from inpatient to outpatient treatment modalities in healthcare. In the post-DRG environment, business offices that were configured for large inpatient per claim revenue re-engineered to support high volume, low dollar outpatient claims submission and follow-up – not an easy task.

According to the HIMSS Medical Banking Project, potential savings in medical banking are over \$35 billion annually, elevating medical banking models from a commercial opportunity to one that requires serious policy consideration. Consider that in 2002, the hospital segment provided over \$21 billion in uncompensated care. It may be possible that banks can convert digital savings in administrative costs into charitable resources for healthcare. So we believe there are significant social dimensions as well, which is to be expected in any significant change in healthcare operating practices. For example, as the rolls of un/under-insured increase, substantive venues that yield better results for our dwindling healthcare resources will be put to the test. Specialized cash management services offered by banks fit this description.

A core concern is clearly medical records privacy, security and transactional compliance. I believe that is more likely than not that more PHI will flow through banks. Accordingly, healthcare policy can be broadened to incorporate a cross-industry approach towards supporting reduction of administrative costs. This necessarily includes the banking stakeholder.

Numerous examples are portentous of how the medical payments arena is evolving today. Financial institutions are beginning to offer services that extend beyond institutions, (i.e., bank-to-hospital), to include medical consumers as well (i.e., HSA/MSA). These dynamics suggest that HIPAA should be applied equally across all medical banking market structures otherwise we’ll be re-visiting this issue in policy circles until it is.

The HIPAA Compliance Workgroup at MBProject sought to assess the impact of HIPAA on products, services and structures that bridge financial institutions with their healthcare customers. Our work was intended to inform national policy in this emerging area.

The HIPAA Compliance Workgroup was formed by the Medical Banking Project to address certain policy issues that are arising in the intersection of banking and healthcare. The Workgroup hopes to provide information that can inform policy in this complex yet dynamic area. The Workgroup met two times in 2004 to define its mission and goals as follows:

Workgroup Mission

Isolate regulatory risk areas and develop responsive policy standards for banking services that involve health data management

Goals

- Determine the likely banking and financial services areas that are impacted by HIPAA
- Identify medical records privacy regulations, such as HIPAA, GLB, FACTA, etc., and provide clarification on privacy gaps and coverage
- Create an assessment framework for determining when banks are HIPAA-defined covered entities (clearinghouses), highlighting areas that require further policy input and/or research
- Develop a standard template for the HIPAA Business Associate contract for banks and/or financial institutions that will accommodate evolving legislative and policy changes
- Define the probable environmental impact of multiple legislative drivers on bank-based healthcare services
- Outline and propose a potential HIPAA bank-based clearinghouse accreditation program (completed)

Background

HIPAA is accelerating a digital payment and remittance environment. Other healthcare transactions are also being targeted by banks (i.e., eligibility). Increased PHI movement among banks is inevitable. As this occurs, various industry models that have been put forth in the literature (i.e., Data mining of Automated Clearinghouse House [ACH] transactions, Financial Electronic Data Interchange [FEDI], Straight Through Processing [STP]) underscores a potential need to assure public confidence when banks handle personal health information.

Banks have a long history of protecting confidentiality and assuring privacy. Indeed, some of the strictest privacy and security standards in the world are maintained by the banking community. HIPAA's privacy and security regulations support this tradition by implementing procedures that enhance public confidence in medical banking market structures.

Section 1179 Debate

Yet an issue that has caused considerable controversy in the industry revolves around financial services that are provided to covered entities under HIPAA. Section 1179 of the HIPAA statute has become a central focus in this debate.¹³ To what extent does section 1179 apply to banks? Does it exempt banks altogether from compliance with HIPAA?

The purpose of HIPAA's Administrative Simplification section was to improve the Medicare and Medicaid programs and to also improve "the efficiency and effectiveness of the health care system, by encouraging the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information."¹⁴

Realizing that "electronifying" personal health data could lead to privacy and security issues, Congress required HHS to submit to the "...Committee on Labor and Human Resources and the Committee on Finance of the Senate and the Committee on Commerce and the Committee on Ways and Means of the House of Representatives detailed recommendations on standards with respect to the privacy of individually identifiable health information."¹⁵ Per direction from the Congress, HHS undertook this assignment in consultation with the National Committee on Vital and Health Statistics¹⁶ (NCVHS) and the Attorney General.¹⁷ Congress specifically sought policy regarding the following issues:

- (1) The rights that an individual who is a subject of individually identifiable health information should have.
- (2) The procedures that should be established for the exercise of such rights.

¹³ 42 U.S.C. § 1320d-8: "To the extent that an entity is engaged in activities of a financial institution (as defined in Section 1101 of the Right to Financial Privacy Act of 1978) or is engaged in authorizing, processing, clearing, settling, billing, transferring, reconciling, or collecting payments, for a financial institution, this part, and any standard adopted under this part, shall not apply to the entity with respect to such activities, including the following: (1) The use or disclosure of information by the entity for authorizing, processing, clearing, settling, billing, transferring, reconciling or collecting, a payment for, or related to, health plan premiums or health care, where such payment is made by any means, including a credit, debit, or other payment card, an account, check, or electronic funds transfer.

¹⁴ *ibid*, Section 261

¹⁵ *ibid*, Section 264

¹⁶ The National Committee on Vital and Health Statistics ("NCVHS") was established under section 306(k) of the Public Health Service Act (42 U.S.C. 242k(k)).

¹⁷ 42 U.S.C. § 264

(3) The uses and disclosures of such information that should be authorized or required.¹⁸

The statute defines individually identifiable health information as

“...any information, including demographic information collected from an individual, that-- (A) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and-- (i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.”¹⁹

While section 1179 exempts payment activities, remittance data, which links an individual with healthcare procedures, is not exempted. HHS draws a clear line between the transfer of funds data (i.e., amount, routing number, etc), and a transfer of remittance data (i.e., the explanation of benefits that often contains medical codes and procedure descriptions). Note the HHS commentary:

“...a covered entity may conduct the electronic funds transfer portion of the two payment standard transactions [820 and 835] without restriction, because it contains no protected health information. The protected health information contained in the electronic remittance advice or the premium payment enrollee data portions of the transactions is not necessary either to conduct the funds transfer or to forward the transactions. Therefore, a covered entity may not disclose the protected health information to a financial institution for these purposes.”²⁰

HHS clarifies this policy as follows:

“The transmission of both parts of the standards are payment activities under this rule, and permitted subject to certain restrictions. Because a financial institution does not require the remittance advice or premium data parts to conduct funds transfers, disclosure of those parts by a covered entity to it (absent a business association arrangement to conduct other activities) would be a violation of this rule.”²¹

Legislative History

According to the legislative history, section 1179 was drafted and lobbied into the statute by credit card processing firms to ensure that HIPAA would not impact the channels set up to efficiently process credit cards, ATM cards, personal checks and other “point of service” instruments that utilize financial clearinghouses. Essentially, a consumer that used such an instrument opted to disclose his or her personal information to the extent provided in the transaction (i.e., the name of a provider on a check); expressly for the purpose of processing a payment.

A payment that flows from a health plan to a provider, however, is different. HIPAA permits disclosure for “consumer-conducted financial transaction,” however remittance data provided from a health plan to a medical provider or a patient is different and used for a different purpose. The “EOB” typically details

¹⁸ *ibid*

¹⁹ *ibid*

²⁰ 65 *Federal Register* 82462, 82496.

²¹ 65 *Federal Register* 82462,82616.

medical procedures that were either fully or partially reimbursed or not reimbursed at all. This information establishes the nature of follow-up for procuring payment of a medical claim and is also used to appropriately apply payments into the medical provider’s accounting system.

Framers of the HIPAA and GLB regulations acknowledged the potential for policy convergence and indicated cooperation if this occurred. Title V of Gramm-Leach- Bliley (GLB) may, or may not, protect a *subset* of the PHI flowing to a bank. The bank is obligated to protect non-public personal information (business information is not included) of its “consumers” (those applying for the bank’s services) and “customers” (those using the bank’s services). Much of the PHI flowing through a bank will not be subject to protection in either category; for instance, when a patient uses a bank not used by the hospital. In other words, the patient’s EOB, containing HIPAA-defined PHI, is sent to the bank that the provider uses for lockbox processing...and that bank may never be used by the patient. HIPAA on the other hand, protects all PHI flowing through the bank via a business associate contract with a covered entity, or via direct federal oversight (i.e., when the bank is a covered entity).

Findings

To the extent that PHI accompanies electronic funds transfers, banking organizations conducting the transaction may need to assess HIPAA-defined risks. Banks that process payment transactions: (1) for covered entities (i.e., provider, health plan); (2) that include *remittance data*; (3) with the exception of “consumer-conducted financial transactions;”²² should assess the impact of HIPAA on operations. In these cases the bank may be required to enter into a business associate agreement with their healthcare client. We note however that HHS will provide further clarification on this issue in future guidance.

Banks that use a subcontractor, including ACH operators, to process funds are likely obligated by the business associate contract to assure HIPAA compliance regardless of the payment channels utilized, whether proprietary, local, regional, national or international. These channels require further review to determine any gaps with respect to HIPAA privacy and security.

Summary of Areas of Impact

The graph highlights potential areas of HIPAA’s impact on banking services. (*Legend: TCS=HIPAA Transaction and Code Sets Rule; P=Privacy Rule; S=Security Rule*)

<i>Common name of banking service or function</i>	<i>Services Description</i>	<i>Short List of Key Risk Areas</i>	<i>TCS/P/S</i>
Cash Management	Banks provide cash disbursement services for health plans that span from receiving a file that is converted into paper checks and mailed to comprehensive accounts payable services that include conversion of	ODFI. Banks have access to PHI when creating electronic payment files with medical remittance information. The X12N 835 is “hybrid” – in that it can contain just	TCS/P/S

²² 45 C.F.R. § 160.103; 65 Fed. Reg. 82,476

	a health plans' payment file to the HIPAA-mandated 835 transaction for processing through the ACH Network. In some cases, the health plan outsources its entire AP area to a bank, so that EOB/EOP data is prevalent in paper and electronic form.	<p>payment data or remittance data, or both.</p> <p>ACH. When the ODFI utilizes an ACH Operator to process funds that contain PHI (i.e., a CTX transaction that contains the full X12 835 – Table 1 and Table 2 data), the subcontractor should likely comply with HIPAA per the requirements of a business associate contract.</p> <p>RDFI. When a receiving bank translates a NACHA transaction (CTX) into a proprietary format for the healthcare provider, it is performing a clearinghouse function.</p> <p>Regardless of revenue, remittance data is protected under the Security Rule.</p>	
ACH networks	<p>A series of financial clearinghouses that function cooperatively to receive and deliver electronic funds transfers messages.</p> <p>The services in this arena include billing, settling, collecting and auditing payments, as well as other services.</p> <p>When these terms are used in the medical arena, we tend to think of medical claims collection, billing, etc. This is not the case in the financial arena, where payment instruments, like debit instructions or checks, are validated, audited, billed to the appropriate bank account and settled.</p> <p>"Net settlement" occurs in between banks and refers to the difference between the value of outgoing and incoming payment instructions for a given batch of payments for a given bank.</p>	<p>Does HIPAA exempt the ACH network under Section 1179? If so, the following points are mute.</p> <p>The "ACH network" is really a series of financial networks, up to 40, with the largest being the Federal Reserve. These systems are supported by a diverse array of vendors who routinely have access to, use and store ACH transactions data. ** Within this context, the HIPAA Security Rule eliminated the term "open network". Does this affect how HIPAA impacts security of this network?</p> <p>** NOTE: GLB and HIPAA protect different classes of information. Regulation P and HIPAA refer to different classes of information.</p> <p>NACHA Operating Rules require that ACH transactions be stored for one year for auditing purposes. This includes medical payments that contain PHI.</p>	P/S (?)

<i>Common name of banking service or function</i>	<i>Services Description</i>	<i>Short List of Key Risk Areas</i>	<i>TCS/P/S</i>
EDI Payments Processing	<p>This service area can be a subset of cash management service. In this discussion, it refers to originating payments for health plans, as well as concentrating incoming electronic payments for health care providers.</p> <p>"Originating" means sending an electronic funds transfer to the ACH network.</p> <p>As noted, this functional area also encompasses electronic payments and remittances coming into a receiving bank (the medical provider's bank). Bank personnel processing incoming ACH transactions (CCD, CCD+, CTX), Fedwire and other electronic transactions, including:</p> <ol style="list-style-type: none"> 1. "Truncating" the remittance information and deleting it 2. Sending all ACH transactions to an external resource for data mining 3. Conversion of all electronic remittances to 	<p>Transmission standards – the use of encryption was made an addressable implementation specification under the Final Security Rule. When banks transmit data that contains PHI to a medical customer, what is the Security Rule requirement?</p> <p>Would this rule apply differently for a bank that is a HIPAA-covered entity (as a result HIPAA-defined clearinghouse functions) vs. a bank that is a business associate of a covered entity?</p> <p>What are the transmission requirements for electronic medical payments containing PHI that are originated by a bank to the ACH Network?</p>	TCS/P/S

	the HIPAA-mandated standard to create a consolidated file for delivery to a medical customer.		
Lockbox Processing	<p>A funds consolidation outsourcing agreement that contractually authorizes a bank to open all incoming mails in a PO Box set up for the purpose of collecting payments (separating the revenue stream of a medical client from other mails and expediting payments processing).</p> <p>Lockboxes are largely manual-intensive in the medical arena. Lockboxes have specialized to incorporate technology that images incoming payments, inclusive of EOBs. Some lockboxes utilize software that employs intelligent character recognition routines that fill in EOB data elements into the 835 file format (per requirement in their contracts with medical providers).</p>	<p>Storage of PHI</p> <p>Transmission of PHI</p> <p>Auditing of PHI? What are the standards?</p> <p>Lockbox facilities have a lot of physical assets. What physical safeguards are applicable?</p>	TCS/P/S
Common name of banking service or function	Services Description	Short List of Key Risk Areas	TCS/P/S
Commercial Lending	An emerging issue that is under review by MBProject is the impact of HIPAA on commercial lending. For purposes of this brief report, let's look at one aspect of this issue: assignment of medical receivable as a result of a violation of a loan document (i.e., death of a key partner, liquidity ratios, bankruptcy, etc.). In this scenario, the bank takes possession of the medical provider's physical hardware/software files, in some cases, but in almost all cases, medical receivable is automatically transferred in order to collect funds and repay the obligation. Medical receivable is "PHI-laden"; without PHI, there is no medical receivable.	As a risk reduction strategy, would banks need to implement HIPAA-specified security policies and procedures to assume an asset containing PHI?	P/S

Recommendations

- ⇒ HHS should confirm that “functional assessment” is an accurate risk tool for assessing status as a clearinghouse under HIPAA.
- ⇒ Consumer credit services will surface in importance and accordingly, policy should reflect this in order to support much needed liquidity in healthcare.
- ⇒ CMS should affirm its policies regarding PHI access and use by financial institutions in order to support latent market forces.
- ⇒ Data mining and encryption represent areas that require further policy work.

Discussion:

HHS should confirm that “functional assessment” is an accurate risk tool for assessing status as a clearinghouse under HIPAA.

CMS has developed what we will refer to as the “doctrine of functional assessment” in response to market questions concerning classification of a HIPAA-covered entity. Yet CMS has provided a new condition that raises more questions concerning classification.

While a number of market structures have been referred to as “clearinghouses” – billing services, re-pricing organizations, community health information networks, funds processing networks, bank and non-bank based lockboxes, bank and non-bank based cash disbursement firms, etc. – it is important that as much as possible, a clear policy should be established with respect to this classification.

Although a bank may be a business associate, its classification as a clearinghouse raises the level of business, organizational, transaction and reputation risk. It may determine whether a bank, for example, wishes to engage in certain medical banking services. In simple terms, when a business or entity offers data conversion to or from a regulated transaction standard under HIPAA, the entity is classified as a clearinghouse and is thus directly regulated (as opposed to compliance per a business associate contract).

In the area of banking services for healthcare customers, these type of conversion activities may occur in at least three areas:

- Cash disbursement operations (ODFI)... for example, a health plan that contracts with a bank to execute ACH and/or other payment transactions.
- RDFI operations...for example, a community bank that converts ACH-formatted electronic transactions – *that contain medical remittance data in Table 2 of the X12 835 transaction* – into a proprietary format that is negotiated with the customer.
- Lockbox operations...for example, wholesale operations that offer character recognition services that reformat incoming paper EOB/P information into an output file structure that is based on the ASC X12N 835 transaction standard implemented by HIPAA’s Transaction and Code Sets regulation.

A closely related policy issue has emerged in the banking arena, but with applications in other industries, that needs to be carefully assessed. Consider a bank that offers services that include a HIPAA-defined conversion function. The bank determines to engage a third party, HIPAA-defined clearinghouse provider (“ABC Clearinghouse”) for this function - it does not provide the function in-house.

The bank wishes to provide an array of services through a single contract with the healthcare customer. The bank does not facilitate a direct contract between “ABC Clearinghouse” and its clients. The contract is between the bank and its client and, as PHI is accessible, the contract contains HIPAA-required privacy and security provisions. The information is as secure as it would be otherwise through a business associate contract.

Clearly, under the “doctrine of functional assessment”, the bank is not operating as a clearinghouse in this scenario. The bank is solely acting as a conduit for HIPAA-defined clearinghouse services. In doing so, the bank makes available multiple service offerings through its single contract with the customer.

We note that CMS has taken the position that if the bank does not facilitate direct contractual relations between its clients and ABC Clearinghouse, the bank is considered a clearinghouse even if it fails the “functional assessment” test – it is not doing the functions that would classify the entity as a clearinghouse. The workgroup seeks to persuade CMS to reverse this opinion. We are unclear as to how this interpretation is legally enforceable and/or how it is derived from the statute and subsequent regulations.

From a macro-economic standpoint, we believe this interpretation will reduce the dispersion of HIPAA-supported efficiencies throughout the marketplace. The reputation of a bank is inextricably linked to its ability to service a community – perhaps more so than any other industry.

Commercial best practices have long recognized that keeping client lists confidential and not opening those up to third party contractors is a conservative and preferred approach. Thus if a bank chooses to help its community to implement HIPAA-defined transactional efficiencies, and could reach into rural areas that have been difficult to engage by traditional health data clearinghouses, it would need to ascertain reputational, organizational and legal risks associated with this decision. From a policy standpoint, this seems to work against HIPAA goals.

The consumer-directed healthcare segment is an example of how this interpretation could impede the goals of HIPAA – or at a very minimum, the implementation of Health Savings Accounts. Several banks are seeking to develop proprietary relationships to support HSAs in concert with requests by the Department of Treasury. These relationships would utilize a card that supports HSA transactions, as well as an array of services that include a clearinghouse component (i.e., processing eligibility information).

In doing so, the bank, according to the CMS position, would need to facilitate “clearinghouse contracts” with all clients that enrolled onto the card program. This has the effect of increasing transaction cost and reducing transparency. The bank, for example, could decide to market this product to other banks, and each one of those banks would then be classified as a covered entity under HIPAA, or, turn over their client lists to separate clearinghouse negotiations.

As noted previously, the CMS interpretation of policy is not specific to the banking industry. For instance, in the case of a third party administrator, which is not named a clearinghouse under HIPAA, 900 separate

negotiations between employers would need to occur to comply with this policy interpretation. This appears to substantively increase HIPAA implementation costs without a corresponding social benefit, in that the privacy and security regulations are not being “ducked” or outsourced, but are in fact incorporated via a business associate contract. There is no need to expand the interpretation, and thus classify more entities as covered entities under the statute.

Another workgroup member questioned whether CMS would be willing, or is able to enforce compliance with all the various vendors that would thus become covered under such an interpretation. This could include a value chain that incorporates variable imaging printers, for instance, or others that while complying with HIPAA privacy and security standards, should not be subject to classification as a covered entity.

Yet another concern was raised with existing networks. Would existing correspondent banking networks, and their supporting vendors, be disrupted as a result of such an interpretation. Each member of a value chain that enrolls clients for a service that could in part, be supplied by a HIPAA-defined clearinghouse, would need to assess the new risk and determine to continue to operate within the value chain, or terminate their relationships.

We are asking that CMS re-examine its position related to “contractually-based, covered entity classification.” In the value chains we examined, banks, IT firms and others involved understand they have business associate responsibilities. The data is being protected per the HIPAA standards. But the application of the clearinghouse classification beyond functional assessment could impact the dispersion of HIPAA-driven efficiencies in the marketplace and raise unnecessary barriers that work against national healthcare goals.

Clearly there are any number of community banks that would elect not to offer these services and this disproportionately affects rural healthcare providers. In other words, the interpretation could result in fewer services being offered in rural areas where they seem to be needed the most.

We believe this is a serious policy issue and are asking for a CMS review within the context of the marketplace, typical business practices (engaging third parties but not opening up client lists to those third parties), and the impact on rural healthcare. In addition, the disruption of existing value chains that learn of their new “clearinghouse” classification under the regulation should be reviewed and quantified in terms of macro-economic cost.

Consumer credit services will surface in importance; accordingly, policy should be designed to support enhanced sorely needed liquidity in healthcare.

HIPAA allows use of PHI with appropriate consumer authorization. External to the ACH Network, the community bank often provides credit services based on demographic data collected from the patient. Without these funds, liquidity for care giver operations will be impacted.

We believe that it is essential to apply HIPAA and other regulations in a manner that does not impede the development of credit services. Indeed, access to, and quality of healthcare is in large part dependent upon the availability of healthcare financing. For example, a hospital that offers patient financing through a bank will likely need to score individuals to determine if they are eligible. In some cases, this type of financing can be done using aggregate scoring models, such that all patients at a hospital can take advantage of the program. Yet we see a potential issue with respect to HIPAA's marketing provisions and the new FACTA regulations which could impede the development of consumer financing instruments. Today's hospital environment requires greater, and not less, liquidity, and this is likely to be the case going forward.

We encourage regulators to view proposed regulations from a cross-market perspective. In the areas of privacy and credit, for example, policy could be informed by a cross-industry process that invites the appropriate regulators from the banking and healthcare industries to surface critical path policy issues and make recommendations.

For instance, in a new consumer-directed health plan environment, banking agencies may point towards the FACTA as providing the necessary regulatory safeguards for medical records privacy and security. But how does CMS view this, especially within the context of the section 1179 exemption of consumer-initiated financial transactions?

**NOTE: This issue represents a clearly identified area where a cross-industry regulatory commission (in healthcare and banking) could assist in policy development. – MBPROJECT)*

We should mention one more item under healthcare credit practices in general that banks and others provide to healthcare providers. An exhaustive study was conducted in this area. The issues are complex and need to be carefully reviewed by policy makers. At the heart of this series of issues is the lending contract that uses healthcare receivable as collateral. Healthcare receivable is PHI-intense; you can't really have a healthcare receivable without the underlying PHI. Thus when a healthcare provider violates the lending contract, the lender has full authorization to take over the receivable...yet this leads to a very complicated series of risks under the HIPAA construct, including unauthorized transfer of PHI. As mentioned, there is an exhaustive study of this issue that can be supplied to NCVHS.

CMS should affirm its policies regarding PHI access and use by financial institutions in order to support latent market forces.

The OCC is clear about what banks can engage in. CMS should be equally clear in asserting its role for overseeing medical banking market structures. For example, the OCC provided this Conditional Approval to a national bank that was seeking clarification regarding whether processing health information is a permissible banking activity:

“The OCC has long recognized that the transmission and handling of medical and health insurance data in connection with activities such as funds transfers, billing services, or claims processing, is an activity that is incidental [to] the business of banking.” [brackets supplied]

In another Conditional Approval, the OCC again outlines its views:

The OCC has determined that a wide range of insurance-related administrative services are authorized for a national bank or its operating subsidiary. It is well established that national banks may provide billing, collection and claims-processing services as an activity incidental to the express authority to engage in processing payment instruments. See Interpretive Letter No. 712, reprinted in [1988-1989 Transfer Binder] Fed. Banking L. Rep. (CCH) 81-027 (February 29, 1996); Interpretive Letter No. 718, reprinted in [1988-1989 Transfer Binder] Fed. Banking L. Rep. (CCH) 81-033 (March 14, 1996). Billing, collection and claims-processing services may include collecting and processing insurance premiums and processing insurance claims. See Corporate Decision No. 98-13, supra. Handling medical and insurance data in connection with these activities is also authorized. See Conditional Approval No. 282 (July 31, 1998).

Clearly, banks are permitted to process what HIPAA defines as protected health information. The existing CMS policy permits this activity so long as a business associate contract is in place with a covered entity and/or the bank, as a HIPAA-defined covered entity, complies with the HIPAA statute and regulations.

While this seems clear, the various interpretations have surfaced that span from full exemption of banks from HIPAA to partial exemption. An indicator of this is the letter drafted by NCVHS which requested clarification from HHS on when a bank should be considered a business associate, as well as seeking resolution on the use of encryption as PHI flows through the financial institutions.

From a macro-economic view point however, we believe that HIPAA policy has shaped market forces in a positive direction. More banks are specializing their services to meet the unique needs of the healthcare industry. Yet medical banking constituencies need to know CMS' position so they can move forward with product development and strategic plans.

Data mining and encryption represent areas that require further policy work.

Data mining is becoming a new focal point in medical banking policy. In terms of the consumer-directed healthcare industry, given that Section 1179 clearly exempts “consumer-initiated financial transactions”, it is essential that the key stakeholders agree on how to assure protection of personal health information in consumer payment channels. This area has been targeted by the adoption of FACTA regulations.

As indicated earlier, HIPAA's application to business-to-business *payment and remittance* data transfers should be affirmed by CMS to address data mining concerns that have been posed by various privacy groups.


In the area of encryption, targeted by NCVHS in its letter to HHS outlining the impact of HIPAA on financial institutions, HIPAA regulations provide a framework for security in clearinghouse structures. The NACHA set of industry best practices while substantive, do not appear to meet HIPAA requirements. The relevant standard under the HIPAA Security Rule requires that remittance data *must only be viewed by the intended recipient*. Yet when CTX transactions are exchanged between ACH Operators they are de-encrypted and then re-encrypted in order to ascertain appropriate routing. While this mostly occurs in an automated fashion, the transactions are stored and available for inspection.

We do not view the fact that ACH Operators have potential access to remittance data for auditing and data mining activities as a HIPAA risk area, to the extent that HIPAA regulations in fact apply to such ACH Operators. Use of the data for auditing is essential to the integrity of the financial system. Likewise, use of the data to support federal, state and commercial purposes is essential to attain efficiency in policy development, product development and other areas. Yet, the application of HIPAA in these areas seems a societal mandate and in any event, appears fully supported in the applicable statute and regulations.

This cross-industry issue needs to be clarified by CMS. It may be advisable to document the security and privacy issues surrounding ACH channels from point of origination all the way through to the endpoint (i.e., RDFI or RDFI's customer).

Final Recommendations from Third National Medical Banking Institute:

1. Work to get CMS to enforce transaction regulations so that we can learn how to make the end-to-end system work.
2. Create an education campaign for consumers to help them under the EHR/EMR ownership options and associated risks based on the different models.
3. CMS should affirm its policies regarding PHI access and use by banks [payment vs. remittance].
4. Banks need education on how healthcare works.
5. Push for clearer HIPAA guidance with respect to transaction standards.
6. Data mining and encryption represent areas that require further policy work.
7. Consumer credit services will surface in importance – policy should be geared towards this eventuality [FACTA – need to be careful to protect privacy but not impede liquidity].
8. HHS should confirm that “functional assessment” is an accurate risk tool for assessing status as a clearinghouse under HIPAA [The “transparency” issue].



HIPAA policy is accelerating cross-industry market structures that reduce administrative costs in healthcare. This far reaching goal requires the active participation of all healthcare stakeholders. Banks are a key player in this process.

National policy goals are clearly supported through evolving medical banking services. By applying HIPAA regulations and guidance evenly across medical banking constituencies, this dynamic can continue to grow, otherwise, new policy interpretations could derail the significant progress we are making as a society in healthcare financing and operations by engaging the banking stakeholder.

WORKFLOW AUTOMATION COUNCIL WORKGROUP

The Workflow Automation Council was formulated to explore ways that banks can automate and/or add value to the workflows in the revenue cycle process. It builds from work that was done at the first and second Medical Banking Institutes.²³ The Goals are to:

- **Map the entire healthcare revenue cycle process**
- **Highlight areas in the revenue cycle that could be improved by introducing banking technologies and infrastructure**
- **Outline corresponding impact**
- **Make industry recommendations**

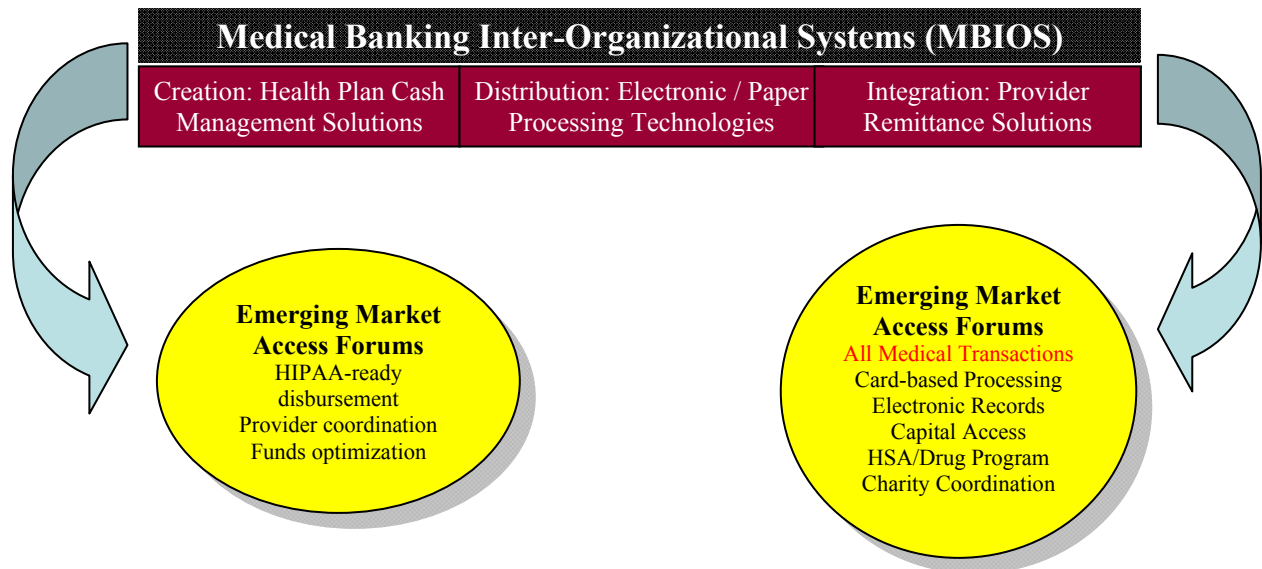
The Workflow Automation Council is an independent, vendor-neutral, collaborative forum that is intended to facilitate dialogue on best cross-industry practices and model development. The Council explored new technologies, business processes, marketing issues and organizational design. A key goal is to explore potential ways that banks can engage and/or rearrange core competencies in a way that helps providers of all sizes to take advantage of electronic healthcare.

The Council, sponsored and organized by the Medical Banking Project, created a high level Working Paper to stimulate cross-industry dialogue among participants. The document does not represent an official position of the workgroup members.

The administration of healthcare typically involves paper intensive processes that lead to processing errors, unnecessary costs and denied claims. Healthcare organizations are increasingly targeting the revenue cycle as an area ripe for process improvement and automation.

As a natural aggregator of payments and remittances, banks are in an excellent position to be able to offer products and services that can improve revenue cycle technologies and processes. In fact, as a middle layer in between financial transaction, the banking community has the potential to implement systemic improvements for both payors of healthcare services and healthcare providers. This includes business-to-business and consumer-to-business transactions.

²³ The First National Medical Banking Institute was held during the 5th National HIPAA Summit in Baltimore, MD. A number of regulators with CMS, the Office of Civil Rights, the Office of the Currency Comptroller, former senior counsel for the Federal Reserve System either presented or attended. In addition, we received support from the Healthcare Financial Management Association's HIPAA@Work Task Force, patient accounting executives from regional healthcare systems and others.



A case study of how banks can help can be demonstrated by industry reaction in 1992, when Medicare provided financial incentives for healthcare providers that were tied to electronic receipt of the ASC X12 835 medical remittance transaction. Providers that made provisions to receive the remittance electronically were offered speedier funds turnaround – a cash flow windfall considering that 40% of the average provider’s revenue are derived from Medicare. The federal government offered free software that “phoned” the Fiscal Intermediary’s IT system, retrieved the electronic remittance advice and then facilitated printing of the files at the provider’s site (“PC Print”).

Within a short period of time, a new series of best practices emerged in the marketplace that focused on automated cash posting of the complex medical remittance. Almost immediately, however, this market evolved to automate far more than cash posting. In fact most of the downstream, paper-driven processes in healthcare were automated as well, translating

Serial View of Patient Accounting Functions	Estimated Manual Cost	Digital Cost
Cash posting	\$1.25	
Contractual Allowance Processing	\$2.50	
Reject Note Posting	\$1.25	
Financial Class Updates	\$1.25	
Secondary Billing	\$5.00	
Patient Statement Processing (series)	~ \$5.00	
TOTAL COSTS	> \$15	< \$5.00
EST. SAVINGS	A minimum of \$10.00	
ANNUAL INDUSTRY SAVINGS	\$20 - \$35 billion	

into enterprise-wide benefits. Notably, this was only enabled for the Medicare segment of the provider’s revenue. See the graph below for a depiction of the potential for savings, which MBProject estimates to be \$35 billion annually. We believe this level of savings raises policy issues.

Today, HIPAA is facilitating a digital environment that can extend efficiencies that have been proven and are now operationalized, for all the remaining provider revenue classes. But how will these efficiencies be accessed? Medicare was a central resource in 1992. What central platform can provide the same critical mass for healthcare today? The only critical mass aggregator of healthcare remittances today is in fact, the bank lockbox. Notwithstanding that HIPAA attempts to shift payments to an electronic environment, the time span for critical mass adoption could mimic the time frame of Medicare – from 5 to 7 years or longer.

In addition, banks have become more educated regarding HIPAA goals and technology requirements. Specialized lockbox platforms can provide a single digital platform for healthcare that offers diverse forms of funds processing (paper, credit/debit card, EFT).

Finally, banks are scoping potential opportunities in healthcare to leverage considerable investments in real time transaction processing architecture to support payments, eligibility, authorization, referrals, claims and the other HIPAA-specified healthcare transaction sets slated for national adoption.

Market Size

National healthcare expenditures are projected to be \$2.6 trillion by 2010 according to the Centers for Medicare and Medicaid Services. The sheer size of this industry, and the fact that all payments move through the banking system, likely means that banks must anticipate the range and rate of business process change in order to develop an appropriate response. This requires further specialization of banking services specifically for the healthcare segment – a relatively recent dynamic in the industry.

Technology

The technologies and business processes used to process payments are undergoing fundamental change. New industry initiatives are fueling this change. This includes the ARC initiative, Check 21, healthcare EDI, optical imaging and advanced recognition, privacy and security regulations (i.e., HIPAA, GLB, European Directive on Data Protection), and the overall movement of administrative areas towards an electronic environment that is transaction-oriented (i.e. real-time processing).

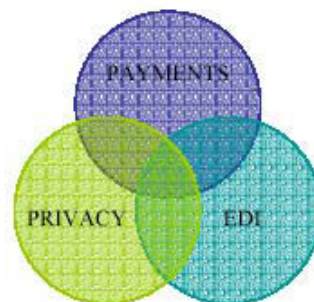
Bank technologies that reduce process inefficiency are emerging, focused on integration along many points of the healthcare complex. This ranges from specialized lockbox services to EBPP to new payment

venues for health plans, integrating card-swipe systems that automate HSA transactions and provide secure access to a patient's medical records and beyond.

The technology formations that are emerging appear similar in nature to the SABRE system (merging online ticket sales with EFT) or Baxter's ASAP system. Like other inter-organizational systems (IOS), new cross-industry IT linkages that merge healthcare administrative operations with payment and remittance processing have the potential to change the competitive rules among banks seeking healthcare clients. A recent series of press releases by leading banks demonstrates this new reality (PNC, BofA, BankOne, ABN AMRO, etc). Thus a market-driven dynamic has been unleashed that will continue to drive this area.

Regulations

The greatest single contributor in terms of policy today that is spurring change in banking and payment systems is the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA implements a series of new federal regulations that need to be examined within the domain of payments processing. The administrative regulations encourage industry-wide adoption of both procedural practices and electronic data interchange (EDI) standards when transmitting payments electronically.



The rate and range of change in this area requires a cross industry perspective in order to identify efficiency opportunities in banking. This requires an understanding of the typical business processes, and supporting technologies, that are used to execute and manage a healthcare payment, from point of claims origination to final resolution.

It is inevitable that as banks engage this area, financial services will be re-scoped to accommodate a wider range of business processes in healthcare. This follows the typical industry patterns that have been documented in the literature.²⁴ An example of this is Metavante's healthcare card product line. The card will link an HSA account, the MasterCard settlement system and United Healthcare's eligibility database. One card swipe will check the patient's eligibility, determine the deductible and process it, as well as provide claims data for adjudication by United Healthcare – with final result being deducted from the HSA account.

The areas of synergy between banks and healthcare that the workgroup considered in preparing this report include technology, infrastructure and credit.

²⁴ IT-Enabled Business Automation: From Automation to Business Scope Redefinition, Sloan Management Review, Venkatraman, 1994.

- *Technology*...refers to the electronic information management systems, processes and automated techniques that have been developed, or are under development by financial institutions and/or their supporting vendors; mostly used to support administrative functions.
- *Infrastructure*...generally refers to physical structures like ATM locations, branch delivery networks, kiosks and other platforms (POS terminals) that are used by financial institutions to acquire transactions volume or to otherwise manage business operations.
- *Credit*...refers to the core competencies of the banking system to efficiently manage corporate and consumer credit, and the new methods of integrating this capability in emerging medical banking platforms.

The workgroup decided to create a process map that shows the revenue management cycle, starting from claims creation to final claims resolution. For purposes of this report, the workgroup utilized a framework that was created by a workgroup member, the Council for Affordable Quality Healthcare (CAQH). Other sources were also used. While the framework provides a portrait of healthcare provider functions, the group also sought to connect payer functions. In between these stakeholders are banking/financial organizations that process payments. While the work is by no means exhaustive, we hope it can provide a basis for further analysis in the area of medical banking workflow automation.

CAQH Framework (www.caqh.org)



- | | | | | | | |
|---|--|--|---|---|---|---|
| <ul style="list-style-type: none"> • Patient inquiry • Appt scheduling • Scheduling verification • Financial review of pending appts. • Encounter form/ medical record preparation | <ul style="list-style-type: none"> • Registration & referral mgmt. • Admin & medical record preparation • Patient visit • Ancillary testing • Charge capture • Prescriptions | <ul style="list-style-type: none"> • Scheduling & referral mgmt. • Admin & medical record preparation • Inpatient care • Ancillary testing • Charge capture | <ul style="list-style-type: none"> • Scheduling & referral mgmt. • Admin & medical record preparation • Surgical care • Post care • Follow-up care | <ul style="list-style-type: none"> • Visit orders & instructions • Education materials • Prescriptions • Ancillary tests • Referrals • Follow-up visits | <ul style="list-style-type: none"> • Utilization review • Claims/bill generation • Billing • Payment processing • Claims follow-up | <ul style="list-style-type: none"> • Personnel management • Financial management • Managed care • Information systems • Facilities management • Medical staff affairs |
|---|--|--|---|---|---|---|

The workgroup utilized the categories of “general operating areas” that were specified in the CAQH framework as follows:

- **Pre-Visit**
- **Office Visits and Other Visits**
- **Inpatient Activities**
- **Post-Visit Follow-Up**
- **Administrative Follow-Up**
- **Administrative Responsibilities**

Sub-activities corresponding to each general operating area were charted. For example, under “Pre-Visit” we charted patient inquiry, appointment scheduling, etc., as shown on the graph below. Finally, each activity was examined within the context of relevant issues, best practices and potential banking opportunities. We note that there may be areas of overlap among general operating areas. The series of graphs that follow provide a summary of preliminary conclusions related to bank opportunities. Many of the findings revealed the potential aggregation of business practices onto a single platform – mainly the card system.

General Operating Area: Pre-Visit				
Patient Inquiry	Appointment Scheduling	Scheduling Verification	Financial Review of Pending Appointments	Encounter Form and Medical Record Preparation
Issues				
No shows, overbooking	Appointment availability	Accurate and timely insurance verification	Identify patient balance and obtain payment	Family medical history, prescriptions utilized
Best Practices				
Electronic Access	Online Scheduling	On-line demographics	Online updated financial information	Online EMR
	Online Eligibility	Standardization of Information		
	Online Referral Management			
Banking Opportunities				
		Health card for automated real-time insurance verification	Health debit card to identify co-pays and deductibles and automated debit.	Health card that contains patient health information
A POMIS distributed by bank that provides single gateway for medical and financial transactions, as well as provider’s internal banking interactions. Could encourage more physicians to engage e-commerce vs. paper claims.		Card program that integrates financial management (HSA, debit/credit); positive identity (reduce fraud); loyalty programs.	Card simplifies collection of patient balances via monthly credit program and includes statement fulfillment services, EBPP and other payment options.	Health card that provides positive identification and permits secure access to a portal with patient’s medical record; versus the entire medical record on the card.

Pre-Visit Summary: In the pre-visit area, banking opportunities center around consumer areas where banks can offer expertise in real time transaction processing and architecture, as well as new models that offer, for example, the new physician in a community a “lifestyle package” that incorporates a POMIS, personal and business credit, medical and financial transaction processing and perhaps other areas.

General Operating Area: Office Visits and Other Visits				
Registration and Referral Management	Administrative Medical Record Preparation	Patient Clinical Visit	Ancillary Testing	Charge Capture
Issues				
Timely authorization and tracking. Need auth # in collection effort otherwise, claim is often pended. Many denials caused by incorrect coding/ insurance/referral info. Potential A/R capture is lost by not collecting the appropriate co-pays/ deductibles.	Collection of all medical record documentation in a timely manner. Manual preparation of Encounter Forms.	Correct / complete documentation	Prepare referrals; obtain authorization. Payers can refuse payment if these tasks are not correctly performed.	Perform correct coding, verify insurance info and enter charges. Obtain appropriate signatures. Claims auditing can reduce fraud & abuse issues. This involves checking claims against Medicare CCI, LMRPs, other; a process that can be automated.
Best Practices				
Standardize referral processes	EMR			
Online real time registration	Online prescription history	Online verification of coverage.	Online testing, authorization, certification, referrals	Standardize all data elements. Use PDAs to enter charges.
Accurate insurance verification				
Online co-pays/deductible information				
Banking Opportunities				
Health card can move authorization transaction.	n/a	n/a	n/a	n/a; charge auditing, however, is an area that should be reviewed.
Card can automate eligibility, provide accurate financial information, and enable patient to pay via debit /credit card	Card can contain correct prescription history.			Provide correct online contract management information.

Office/Other Visit Summary: The majority of banking opportunities in this area continue to focus on a card platform. However the comments also suggest that links to databases that can automate contract management and/or code auditing surface as a potential cross-over model for banks. A key reason why these areas are relevant is due diligence for making credit determinations. CMS reported that over \$20 billion was overpaid by Medicare in 2003. In some credit arrangements, it may be important for the bank to monitor this issue.

General Operating Area: Inpatient Activities				
Scheduling and Referral management	Administrative and Medical Record Prep	Inpatient Care	Ancillary Testing	Charge Capture
Issues				
Obtaining correct referral and authorization. Can lead to denied claims if incorrect information. Lost revenue in not identifying proper co-pay/deductible at time of service	Capture correct information and consults. Document prescriptions, consult requests	Document care and charges	Obtain correct authorizations	Complete encounter forms, obtain eligibility, input correct charge codes. Validate coverage
Best Practices				
Automate referrals. Set up pre-registration unit to capture info prior to visit. Enable multiple payment options such as on-line payment, debit card payment.	Enable documentation via PDA. Implement standardized consult process.	PDA documentation	PDA Documentation	Automated eligibility checks. Smart card containing real time patient eligibility info
Banking Opportunities				
If bank integrates online POMIS system to its service features, this can be a revenue source, as well as revolutionize access to technology by solo providers.	n/a	n/a	n/a	n/a
Automate eligibility and referrals via partnerships. Enable online payment via ach/credit card. Offer debit card.	n/a	n/a	n/a	

Inpatient Activities Summary: This area significantly overlaps functional areas already examined in the Office/Other Visits area. Once again, a smart card is named as a potential resource that can enhance automation and payment transactions.

Some financial organizations have commented on the area of “administrative and medical records preparation” with respect to data capture from paper records. Banks have invested in a wide range of specialized architecture and technologies that efficiently support document management, archiving and complex research routines. This area will need to be reviewed further as electronic medical record technologies stabilize and/or as a certified body of best practices begins to emerge.

General Operating Area: Post-Visit Follow-Up			
Visit Orders and Instructions, Education Materials	Prescriptions	Ancillary Tests	Referrals
Correct orders.	Accurate prescriptions. Know patient history.	Obtain correct certifications/referrals.	Schedule follow-up visit. Write appropriate referral. Obtain certifications. Send referral forms to the business office.
Online educational materials/orders	PDA for prescriptions.	EMR	Automated referrals. Tracking systems.
n/a	Banks can help to distribute prescription cards, as well as to manage transactions. This is opportunity in 2004-2005 time frame (about \$17B) and can be used as a lever in 2006 when MMA kicks in w/major drug benefit of \$400B.	n/a	n/a
n/a	Prescription cards containing patient history and payment capability.	n/a	n/a

Post-Visit Follow-Up Summary: One of the areas that has been targeted by CMS is the prescription drug benefit. In the program, an individual can gain access of up to \$1,200 in 2004-2005 to assist in the payment of prescription drugs. CMS chose a card format for complying with the entitlement. The program has not been as widely used as anticipated and CMS has asked financial institutions for recommendations in this area. Financial institutions have created efficient, secure and scalable process to issue cards and acquire financial transactions. The ability to utilize existing technologies and architecture to program a stored value card, in conjunction with a PBM company, for instance, could yield a new format that can be mass marketed. In this area, there is not equivalent industry that can provide mass outreach and increased utilization. The same card that is used in this program could be layered with additional functions, as indicated in the card features related to other operating areas.

Another functional area related to the card that is being examined by some of the world's largest financial organizations, is its use for gaining secure and confidential access to a person's medical records. This process and architecture has yet to be designed, however, we note that other banking organizations in the world have designed this capability. Noteworthy are projects in Australia and South Africa.

General Operating Area: Administrative Follow-Up				
Utilization Review	Claims and Bill Generation	Billing	Payment Processing	Claims Follow-up
Issues				
Pre-certification. Obtain Certificate of medical necessity.	Missing information creates denials, can be very manual.	same	Manual process, matching of payments to remits, inaccurate coordination of benefits, manual secondary billing	Manual process. Denials management.
Best Practices				
On-line UM, certification. Automate medical necessity.	Automate claims submission, electronic submission	Clearinghouse, standard transactions. Automated referrals.	Utilize electronic 835s to automate posting. Utilize lockbox. On-line coordination of benefits. Contract Management system.	On-line electronic remits (835). On-line EOBs. Standardized denial codes. Follow-up system to automate process. Automated denial tracking tools and secondary billing.
Banking Opportunities				
n/a	Banks can partner with claims firms to offer integrated solution to smaller providers.	Acquire/Partner with clearinghouse to integrate this function in cash management	Divide into easy to difficult areas where banks can assist based on receivable type and processing characteristics	Denial Management and contract management modules can become integrated into the banking system to reduce costs for healthcare providers.
n/a	Offer claims processing services via partnerships with medical billing companies/software companies	Partner with clearinghouse	Payments CH as a value added service to lockbox. Paper payments converted to HIPAA 835. EDI platforms distributed to providers.	Denials management tools can be created utilizing the HIPAA 835 data. Automation of contractual allowances, reject notes, financial class update; and contract management, secondary billing and patient billing.
			Utilize POS Terminals to process deductibles and co-pays in a closed or open loop system.	
			Process 835 and 837 data in a closed loop network.	
			Process deductible, co-pay, Flexible and Health Care Spending Account payment in an open-loop network.	

Administrative Follow-Up Summary: This area can be categorized into front end and back end processes. Real time financial transactions in healthcare can be enhanced using a card program. This will simplify payment via HSA, FSA mechanisms, administer real time claims submission, check for eligibility, etc. These enhancements will improve the front end process and will likely involve financial intermediaries.

Back end process will enhance existing workflows. They will bridge the time from where we are today (i.e., voluminous EOB paper processing) to the real time world where we are moving towards. In many cases, banking technology and infrastructure has been specialized to address vertical needs (i.e., lockbox platform, image capture, OCR). Thus providers can engage a lockbox to outsource its payment processing for both third party payers and consumers.

Yet creating EDI linkages that duplicate the requisite previous or subsequent steps of a business process may not have occurred (i.e., EBPP and/or statement rendering, automating cash posting of commercial and/or self-pay receivable). This creates new product opportunities.

A lockbox transport system can adapt to support a diverse array of consumer credit alternatives in a community. Operational models, from real to theoretical, need to be articulated in order to advance the field of medical payments efficiency.

Finally, the back end category of banking opportunities target high volume providers. Yet with advances in technology, and strategic alliances that have already created electronic systems that are installed in the marketplace, lockbox resources can reach the lowest volume providers. This is partly because of cost per unit reductions. But it also reflects the growing understanding of a bank for using the data flows to create auxiliary products that offer new cash management services, and fee revenues, that can be attractive all the way down to the solo physician segment.

In this manner, medical banking provides an opportunity to extend HIPAA-derived efficiencies all the way down to the smallest market segment, as a cash management offering by the community banker who aggressively seeks healthcare relationships. This dynamic can be construed as a major policy success, among a cacophony of voices suggesting otherwise, related to HIPAA's impact in the marketplace.

General Operating Area: Administrative Responsibilities				
Financial Management	Personnel Management	Managed Care Management	IS Management	Medical Staff Affairs
Issues				
Lost revenue due to improper follow-up of denials. Determination of appropriate 3rd party liable for claim, including other resources to assist payment (charity). Accurate documentation for uninsured status.	Facilities outsourcing is a business, but not one that a bank has ventured into yet.- Casillas	Audit payments on a timely basis.	High cost of maintaining systems. Outdated systems. Various applications not integrated with each other.	n/a
Best Practices				
Online Follow up system. Contract Management system.	Standardization/policies and procedures.	Contract Management system.	Integrated systems. Outsource non-core applications. ASP solutions reduce costs.	n/a
Banking Opportunities				
Some banks considering full A/R outsourcing coupled with improved electronic processes.	n/a	Real time auditing of managed care payments.	Integrated bank product that manage financial and medical transaction.	n/a
Offer high value tools online for contract management, denials management and collection via partnerships	n/a	Comprehensive reporting utilizing 835 payments data. Enable contract management.	Offer outsourced solutions - image archive system to research payment data.	n/a

Administrative Responsibilities Summary: The sub-activities referred to in this area generally represent facilities management opportunities. Generally speaking, banks do not offer facilities management programs for healthcare. Banking opportunities identified in this area focus on improving financial management (denials and contract management) via tools that take advantage of remittance data flowing through lockbox/EDI channels. These new services are generally being offered using an ASP format that shifts IT investment risks away from the provider in return for transaction fees based on use. In this manner, banks can ramp providers onto digital networks that add significant value at a minimal cost.

In addition, banks have created highly efficient imaging and archiving systems that can both provide online access to images as well as electronic files that have been developed using those images (i.e., converting a paper EOB to an X12N 835, flat file or other format). Providers can then automate

remittance management using internal or bank-supplied IT platforms (leased or purchased, based on provider requirements).

Workgroup Observations / Recommendations

Observations:

- ⇒ Banks and financial institutions can reduce healthcare administrative costs by \$35 billion or more annually
- ⇒ Banks are well positioned to provide outsourced solutions that automate revenue cycle processes and reduce processing costs in healthcare billing, posting, follow-up and collections. This includes web-based tools that automate denials and contract management processes and other areas.
- ⇒ In the near term, banking services will support HIPAA policy goals by offering a payments/remittance clearinghouse that enables X12N 835 delivery and integration with the patient accounting systems.
- ⇒ Banking technology will enable providers to increase revenue capture at point-of-service using debit cards that facilitate co-pay and deductibles and other methods. Banks will increasingly configure platforms to accommodate real time processes that support near term (24 hour) turn around of payments for healthcare services.
- ⇒ As banks engage this area, investment risks in administrative IT will shift from the healthcare provider to the bank. This will help providers to focus more resources on clinical excellence.
- ⇒ Banks have significant architectural features that can be leveraged to speed adoption of a regional and national healthcare information network.
- ⇒ New community services enhanced by banking infrastructure will reduce healthcare administrative costs and increase access to healthcare from public, non-profit and private sources.
- ⇒ The potential to integrate institutional and consumer credit using data derived from medical banking platforms will likely result in much greater liquidity for healthcare.

Recommendations:

- ⇒ More research and education is required to address the many facets of this new and promising area.
- ⇒ Pilot programs need to be funded to increase awareness of the potential to reduce healthcare costs using banking resources.

Final Recommendations from Third National Medical Banking Institute

1. More research and education is required to address the many facets of this new and promising area.
2. Pilot programs need to be funded to increase awareness of the potential to reduce healthcare costs using banking resources.
3. Information formation standards need to be developed with support and collaboration among existing standards groups, including healthcare and banking participants, focused initially on the following transactions:
 - a. Eligibility
 - b. Claims Adjudication
 - c. Payment and Remittance
 - d. Others
4. Pilot program should show benefits of integrating the 835/remittance transaction back to the provider for seamless posting to revenue system.
5. Develop policy point of view and consensus on HIPAA and banking.
6. Focus on leveraging banking infrastructure to streamline and automate the collection of co-pays and deductibles at point of service for providers.
7. Develop a model for how banking can support the Healthcare Spending Account product.
8. Educate and engage vendors in the development of the solutions.

**Testimony
by
John Casillas
Chief Executive Officer of BoardTrust, LLC.
to the
National Committee on Vital and Health Statistics
Subcommittee on Standards**

**Hearing titled:
Section 1179 of the Health Insurance Portability and
Accountability Act**

May 6, 2015

Relevant Background

- Medical Banking Project attempted to isolate impact of section 1179 in marketplace (acquired by HIMSS in 2009)
- Section 1179 was the subject of intense and exhaustive outreach to government, commerce and academia
 - 12 national roundtables over 24 months (2001-2003)
 - 13 national medical banking institutes (2002-2013)
 - Numerous policy forums
 - Collectively, we engaged 800+ individuals in:
 - Government (CMS, HHS, OCR, Dept of Treasury)
 - Healthcare providers and large health plans
 - Associations in banking and healthcare (HIMSS, AMA, NACHA, ABA, NGA, etc)
 - Commercial bankers, health IT vendors, policy consultants, university professors and many others

Focus on 3 areas today

1. OCC, HHS and HIPAA
2. Symmetrical application of HIPAA across market structures
3. Evolution of healthcare payment innovations and HIPAA

Focus Area 1

Although the OCC lists traditional health data clearinghouse services as a permissible national bank activity that is incidental to the business of banking, only electronic funds transfers (EFT) appear to be exempted from HIPAA.

- CMS official: section 1179 “was never intended to exclude banks. Period.”
- Lobbyist: testified at NCVHS that section 1179 implemented at request of credit card sector who wanted to exchange funds without the impediment of HIPAA compliancy
- HHS clarifies this policy as follows: “The transmission of both parts of the standards are payment activities under this rule, and permitted subject to certain restrictions. Because a financial institution does not require the remittance advice or premium data parts to conduct funds transfers, disclosure of those parts by a covered entity to it (absent a business association arrangement to conduct other activities) would be a violation of this rule.” 65 *Federal Register* 82462,82616.

Focus Area 1

Although the OCC lists traditional health data clearinghouse services as a permissible national bank activity that is incidental to the business of banking, only electronic funds transfers (EFT) appear to be exempted from HIPAA.

- “The OCC acknowledges that the “business of banking is an evolving concept and the permissible activities of national banks similarly evolve over time.” *Office of the Comptroller of the Currency, Activities Permissible for a National Bank, 2005, p 1.*
- “The OCC has long recognized that the transmission and handling of medical and health insurance data in connection with activities such as funds transfers, billing services, or claims processing, is an activity that is incidental [to] the business of banking.” [brackets supplied]

Focus Area 1

Although the OCC lists traditional health data clearinghouse services as a permissible national bank activity that is incidental to the business of banking, only electronic funds transfers (EFT) appear to be exempted from HIPAA.

- The OCC has determined that a wide range of insurance-related administrative services are authorized for a national bank or its operating subsidiary. It is well established that national banks may provide billing, collection and claims-processing services as an activity incidental to the express authority to engage in processing payment instruments. See Interpretive Letter No. 712, reprinted in [1988-1989 Transfer Binder] Fed. Banking L. Rep. (CCH) 81-027(February 29, 1996); Interpretive Letter No. 718, reprinted in [1988-1989 Transfer Binder] Fed. Banking L. Rep. (CCH) 81-033 (March 14, 1996). Billing, collection and claims-processing services may include collecting and processing insurance premiums and processing insurance claims. See Corporate Decision No. 98-13, supra. Handling medical and insurance data in connection with these activities is also authorized. See Conditional Approval No. 282 (July 31, 1998).

Take aways:

- The OCC is clear about what banks can engage in.
- HHS should be equally clear in asserting its role for overseeing medical banking market structures – innovations at the nexus of banking, healthcare and technology that involve use, disclosure or access to PHI.

Recommendation

- HHS should implement a cross-stakeholder panel of independent experts that can meet on a regular basis to review evolving medical banking policy issues.
- Given the significant and persistent investment by banks into the health IT domain, and the forward focus of electronic healthcare to engage consumers, debates will surface around “policy friction” between these two large industries.

Focus Area 2: Symmetrical application of HIPAA across all market structures.

- 3rd National HIPAA Summit: senior policy advisor at HHS/OCR discussed application of HIPAA to banks. The advisor was very clear: *no sector was omitted from HIPAA*
- Bank-based, health data clearinghouses are now a reality (as envisioned by OCC)
 - HIPAA compliant vs. non-HIPAA compliant “clouds”
 - Was this the intention of the framers of HIPAA?

Recommendation

- **Education and educational materials are needed for the banking community.**

Many in healthcare are already sensitized to HIPAA; not as much among banks. HIMSS, NACHA, WEDI, EHNAC and others are vital for this effort. These groups in particular collaborated on creating a policy document enumerating actions that should be taken to implement a HIPAA compliant operating environment that could become a basis for education.

<https://healthcare.nacha.org/sites/healthcare.nacha.org/files/files/FI%20Compliance%20Guidelines-08102012%20Update.pdf>

Focus Area 3:

Healthcare payment innovation and new forms of healthcare credit, especially as we move towards e/mHealth, will evolve cross-industry policy issues in banking and healthcare.

- The “holy grail” – full automation of HIPAA transactions at point of service, with a swipe
- Reconciling “consumer initiated financial transactions” of section 1179; apply EFT interpretation
- Other “burning” policy issues
 - Responsibilities within a value chain
 - Healthcare credit practices that involve health A/R as collateral

Recommendation

- **Policy executives should actively engage and speak at educational forums that are at the nexus of banking, healthcare and technology.**

Understanding how this market is evolving is vital from a policy perspective as banks address security and privacy across all the payment mechanisms.

Thank you...

John Casillas

CEO, BoardTrust, LLC

615-479-7103