

# DRAFT - ABSTRACT



## HIPAA COMPLIANCE WORKGROUP

© 2005 The Medical Banking Project. All Rights Reserved.

### *Workgroup Members:*

Catherine Warren, CTP, VP of Healthcare Strategy for Global Treasury Services, Bank of America  
Nav Ranajee, VP of Business Strategy, ABN AMRO  
Chad Preston, VP of Sales, Premium Asset Recovery Corporation  
Rick Morrison, CEO, Remetra, Inc.  
Jeff Shapiro, Healthcare Specialist, DP Solutions  
Dr. Maureen Levy, President, Irvine Medical Health Affiliates LLC

### *Sponsor/Organizer:*



320 Main Street, Suite 230  
Franklin, TN 37064  
[www.mbproject.org](http://www.mbproject.org)

### Third National Medical Banking Institute

### *Educational Grantor:*



## DRAFT

### Statement of Purpose

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)

**DRAFT**

**Abstract**

Today's new privacy environment has led to considerable change in banking compliance, regulations and supporting market structures. While the Health Insurance Portability and Accountability Act of 1996 or "HIPAA" is derived from privacy and security risk assessments in the healthcare community, the statute and subsequent regulations have tended to expose new areas of risk in the services that banks provide for healthcare. The bank service areas that HIPAA sheds focus on fall into several banking areas as follows:

- Cash management (lockbox, cash disbursement)
- ACH networks
- EDI payments processing (remittance consolidation)
- Lockbox processing
- Credit management
- Online payments (EBPP and card services)
- MSA/FSA/etc. support
- Data mining

HIPAA has resulted in new banking programs that are specialized for the healthcare segment. 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 banks fill the technology void with internal programs), it is safe to say that the impact of HIPAA on banking services for healthcare appears substantial, pervasive and very 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.

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

DRAFT

Workgroup Recommendations / Observations

- **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 types 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

**DRAFT**

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-

**DRAFT**

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 reputation, 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.

**DRAFT**

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-defined efficiencies in the marketplace and raise unnecessary barriers that work against HIPAA policy and 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. We are asking CMS to review the issue 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.**

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

**DRAFT**

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?

- **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*

**DRAFT**

*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.

**DRAFT**

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, do 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).