

HIPAA Summit VII

Preconference III

Advanced Strategies to Achieve ROI in Implementing HIPAA

Case Study Report: The Health Reinsurance Association (HRA) and Pool Administrators Inc. (PAI)

By Karl Ideman, PAI CEO and HRA Administrator

SUMMARY OF REPORT FINDINGS

Milliman USA's overall assessment of HRA's compliance status revealed that HRA had an extensive number of tasks that had to be completed, which involved all major functions in order to achieve compliance with HIPAA rules and regulations within the mandated timeframe for compliance. These tasks fell into four (4) major areas:

1. ***Operational Policies and Procedures*** – PAI staff developed a significant number of policies, procedures, standards and protocols as a basis for administrative operations and for educating and training its staff on both HIPAA and HRA's compliance with its provisions. The HRA Board of Directors in turn, approved the established policies and procedures to demonstrate and document its commitment to protecting the privacy of each plan participant's health information (Protected Health Information – "PHI"). As a result, the Privacy Project Team drafted and the board approved 47 policies and procedures. The Security Project Team is developing 34 policies and procedures now that the final Security regulations have been promulgated.
2. ***Communications Program***- PAI developed a communication program designed to inform all of HRA's plan participants of HRA's privacy policy, as well as plan participants' rights under both HIPAA and HRA's policies. Additionally, we provided its contracted healthcare networks ("business associates") with HRA's privacy policies. These contracted healthcare networks, in turn, passed that information along to all of their individual providers, as these providers were considered extensions of the Covered Entity's operations.
3. ***"Business Associates" Contracts*** - The general requirements for privacy and security have been incorporated into the Business Associate contracts that Business Associates have signed and included in their contracts with their individual providers. HRA has assured that all of its "business associates" have become HIPAA compliant for Privacy within the appropriate timeframe. The reason for this action by HRA was that HIPAA effectively made it responsible for overall compliance and placed the burden of achieving compliance with the Covered Entity's compliance by its "business associates" as required by the regulations. If any contracted vendor ("business associate") could not assure HRA that it will be compliant within an acceptable timeframe, it may have become necessary for HRA to consider and plan for alternative arrangements in order not to be in violation.

4. ***Electronic Data Interchange (EDI)*** - HRA now needs to become HIPAA compliant and to develop the capability of electronically receiving and transmitting protected health information (PHI) as part of its day-to-day operations. PAI worked with Milliman to complete a more detailed review and evaluation of the possible alternatives for systems remediation (Exhibit A). Functional requirements and EDI mapping of PHI was accomplished with the assistance of Milliman and PAI's current IT staff from MIP Systems. These became the functional and technical criteria (Exhibit B) that were used to compare the costs vs. the benefits of the four alternatives. This effort impacts PAI's IT function, where compliance actions will mostly involve computer terminal access controls, physical hardware security and software application modifications. Specifically, HIPAA requires PAI, as HRA's administrator, to be able to electronically receive and transmit protected health information in all nine published transactions since PAI currently transmits PHI electronically (fax and e-mail). The PAI system requirements are shown in Exhibit B are for 834 Enrollment; 820 Premium; and 270/271 Eligibility/Status transactions only since the remaining transactions requirements are covered by the claims administrators as part of their claim processing functions.

As a result, PAI's IT vendor/consultant, MIP Systems (MIPS) is providing PAI with specific solutions, modifications and upgrades that will allow HRA to receive and transmit in compliant EDI transaction, code sets and identifier standards. The consultant has committed to realistic timeframes and due dates to meet HIPAA compliance standards.

5. ***Facility Privacy and Security*** – PAI also resolved the physical layout and facility issues related to safeguarding PHI for its client. In addition, PAI improved the securing of PHI in files and in other internal and external record retention areas. For example, a records retention policy and its associated procedures have been drafted and reviewed/approved.

Additionally, Milliman recommended that the Board, HRA staff and PAI management give serious consideration to the following HIPAA compliance process recommendations:

1. **Immediately begin the compliance plan development process while the Board and senior management discuss and determine HRA's compliance strategy;** In response, PAI presented the compliance plan including the Transaction strategy which is being implemented in time for the October 16th deadline.
2. **Appoint a Privacy Officer;** In response, HRA named a member of the board as the Privacy Officer and PAI is fully staffing this volunteer with its own Privacy Officer Liaison chosen by the board.
3. **Appoint the Compliance Project Manager who will be responsible for, with Milliman, managing the compliance process, setting and adjusting timetables, working with contracted providers/"business associates," and preparing status reports for senior management and the Board;** The Project Management Office as recommended by Milliman was presented to and was approved by the HRA board at its Annual meeting. A Project Management Committee fulfills the role of Compliance Project Manager. The Committee is chaired by PAI's CEO and includes three Project Team Leaders from PAI senior Management in the areas of Privacy, Security and

Transactions. Milliman and MIPS are also represented on the Management Committee. The Steering Committee of three board members and the Management Committee Chair review and accept key milestone deliverables after they have passed review and approval by the Management Committee which deals with all work products and deliverables.

4. **Appoint an individual to coordinate policy issues between functions and determine the role, authority and scope of that individual's responsibilities;** The Project Management Office as recommended was modified. The Project Management Committee was charged by the board to fulfill the role of Compliance Project Manager, although the ultimate responsibility resides with its Chairperson.
5. **Decide who will be responsible for project oversight and technical assistance, including knowledge of HIPAA's provisions, requirements and solutions as well as providing recommendations on compliance issues and strategies affecting business operations and both internal and external relationships;** In this regard, the Committee is responsible for project oversight. The Project Team Leaders supported by Milliman's HIPAA Consulting Team provide technical assistance and make recommendations on issues and strategies as they apply to both internal and external relationships. This responsibility alignment has proven very successful and the Committee has coordinated the resolution of all policy issues presented to it.
6. **Determine what internal/external resources will be available to the Project Leader and the task force;** The Project Teams has utilized the resources of Milliman to assist in the work for quality assurance and MIP Systems for systems analysis and programming to comply with the EDI requirements.

Begin to develop operational alternatives in areas where achieving compliance may be jeopardized. Complying with the requirements of HIPAA necessitated a diligent and time-consuming effort, over and above the daily operation of HRA. There are minute levels of detail affected by HIPAA's privacy standards that will require some degree of remediation to become compliant. Alternative plans included the use of additional Milliman resources if we fall behind schedule; however, this has not been necessary due to the effectiveness of the planning effort and the quality of the project staffing and overall collaboration.

THE INVESTMENT AND THE RETURN (ROI)

Milliman undertook, as part of the GAP analysis, a more detailed review of the possible alternatives for systems remediation. Milliman evaluated alternative remediation approaches to the HRA systems to become compliant with HIPAA's transaction requirements. Functional requirements and EDI mapping of PHI was accomplished with the assistance of Milliman and PAI's current IT staff from MIP Systems. Milliman's four Transaction Strategy Alternatives: System Replacement; System Remediation; Clearinghouse; and Translation were considered as to costs vs. benefits. PAI chose MIP Systems because its proposed system costs were lower than either of the software vendor packages and lower than Milliman's estimated set up and annual transaction cost of the Clearinghouse option. The Translation option was not considered viable by Milliman or by PAI.

The lower costs came from MIP Systems' ability to design and install only what HRA needs versus an entire package. A possible explanation for the high clearinghouse costs is that they seemed to be designed for claims and didn't separately consider premium and eligibility functions which were the only functions needed by HRA and PAI. After the vendor selection was completed, PAI decided to purchase the new system and to charge back the HRA portion of the costs over five years. PAI also expects that it can expand its use of the system to other pools and thus lower the HRA system costs over time.

HRA is a covered entity with regard to HIPAA and the transaction requirements. As such, if HRA should send or receive certain transactions electronically, HIPAA requires that HRA be able to send or receive such data in transactions that have standardized formats using the standard code sets and unique identifiers promulgated by HIPAA.

PAI administers HRA's business as well as CSEHRP's business, and since both HRA and CSEHRP must comply with the privacy and security requirements of HIPAA, a combined remediation for the transactions as well as privacy and security could be most cost effective. PAI is drafting all policies and procedures so that they are applicable to HRA and CSEHRP in order to avoid unnecessary duplication of work. HRA is a covered entity that is required to become compliant with the HIPAA transaction standards, taking on the remediation of CSEHRP's systems at the same time and in a consistent manner as HRA may reduce the cost of doing the work separately. This coordinated approach for CSEHRP and HRA would allow PAI to efficiently put systems around both CSEHRP and HRA that makes the systems more functional. Our systems analysis tells us that the billing and claims audit functionality for both HRA and CSEHRP can be accomplished using very similar processing and reporting logic.

Analysis of System Alternatives

HRA may elect to follow one of these alternatives or use two or more in combination. The approaches are:

A. System Remediation

This approach involves modifying existing HRA systems to send and receive HIPAA format and content compliant transactions. This would include incorporating HIPAA specified identifiers and code sets with a system's native program operations. Meeting HIPAA standards would also involve modifying data file storage used for current operations and historical reporting. The current three systems are legacy database systems running with simple COBOL programs that have limited data tables and no system interfaces between them. In many cases, however, the legacy systems do not have the necessary interface points to support the full suite of HIPAA transactions.

The HRA Billing Application is the primary means of computerized data collection and storage for HRA. HIPAA standard formats for ASC X12N 834, 270 & 271 are not in place now. The Application will need to be modified or replaced to ensure all data elements are being collected and stored appropriately. Additionally, access to PHI and its dissemination will need to be tracked as required. An EDI facility also needs to be put in place.

B. System Replacement

To implement this approach, HRA will need to determine if its systems are ready for retirement and then to identify replacement options. A replacement approach also requires that the transition period is acceptable given HIPAA's deadlines. Currently HRA has no plans for system retirement, although it has identified servers that need upgrading to ensure that HRA has the capability to handle an expected additional volume of EDI transactions.

The old HRA billing system was abandoned and a temporary individual billing system was installed by MIPS but it is not HIPAA compliant. Other off the shelf group billing systems was not strong in the area of individual billing and this would require modification to meet both group and individual billing needs. In addition, MIPS has proposed a replacement approach that delivers the new system for testing by April 2003.

C. Clearinghouse

HRA's systems are housed with PAI who administers HRA's business. PAI primarily sends and receives data on paper although PAI receives certain reports on computer diskette. A clearinghouse could convert paper information to the standard electronic format and accept electronic information on HRA's behalf. Depending on HRA's preferences the clearinghouse

could convert received information to paper or into HRA's own electronic formats or post the information on an FTP site. Clearinghouses typically charge on a per transaction basis with additional set-up and maintenance charges depending on HRA's requirements—for example, the need to convert standard transactions to HRA's own electronic or paper formats or to install a special front end system. Per charge costs would vary depending on transaction volume and HRA's conversion requirements. Based on our review, we estimate that the typical cost from a clearinghouse would be approximately \$125,000 for set up plus an n 0.50 to \$1.25 per transaction depending on the complexity of the function. PAI's estimate of annual transaction volume produced a range of \$ 50,000 to \$ 90,000 transaction cost plus \$125,000 set up costs in the first year of the clearinghouse option. After considering the above, PAI has decided to have a system built which will suit the needs of the HRA and any state high risk pools it administers in the future. The cost of the System to Pool Administrators Inc. will be approximately \$97,162 to \$131,454. It is the intention of Pool Administrators Inc. to recover the cost of the system over a five year period. The cost to the Health Reinsurance Association, for at least the first year of that five year period, would range between \$24,290 to \$32,864. The cost would decrease as Pool Administrators Inc. starts to administer more state high risk pools, as they would be charged a portion of the system costs.

D. Translation

The translation approach involves using existing electronic formats and converting them to HIPAA standard transactions using a separate utility. Since PAI is currently essentially a paper transaction system for HRA with limited electronic database functionality, there is a lack of capacity for taking advantage of a translation approach. Therefore, translation does not appear as a viable option.

EXHIBIT B

(PLEASE NOTE THAT THE ENTIRE MATRIX IS 40 PAGES SO A FEW SAMPLE PAGES ARE ALL THAT IS INCLUDED IN THE CASE STUDY REORT)

SYSTEM REQUIREMENTS FOR THE PAI BILLING SYSTEM

PAI must have the ability to enroll, supply eligibility determinations and maintain enrollment as part of its day to day operations. The system must have combined participant eligibility data with user defined billing formulas to produce monthly and quarterly bills to groups or individuals. A broad range of benefit plan design and multiple effective dates must be permitted.

Easy-to-use new benefit implementation tools and customizable benefits management tools are needed as opposed to role based benefits management tools. PAI's ability to receive payment for all enrollees for the benefits provided is critical. PAI must have the ability to bill for benefits supplied, to print, mail and post payments from individuals, carriers and other defined groups.

Changes to bills based on late enrollments, retroactive terminations, etc. must be handled automatically by the system. The system must automatically trigger adjustments on the billing invoice and then must adjust any related administrative payments (administrative fees, commissions, etc.) to Business Associates and other third parties.

Claims audit is critical in performing PAI's fiduciary responsibilities. The ability of the software to both receive and have query capabilities against claims detail and summary level claims is critical now. PAI does not currently need to process claims with full auto-adjudication capabilities but there is the need to be sure that the new system can link directly to a fully functional claim system.

The system must create the calculated payables to Business Associates and others with associated accounts payable vouchers. It must create an automated file that will post these entries into the Accounts Receivable and Accounts Payable systems and create entries automatically into the Great Plains General Ledger System. The system must allow staff to enter manual invoices which may be for items other than those coverage categories directly billed.

PAI engages in numerous customer services activities with the subscribers, vendors and other business partners. The system must make the most frequently needed data and document images instantly available to staff. Staff must be able to view information about the group, plan and caller with few key strokes and view or enter notes and correspondence about a participant or claim, and to document phone calls and other interactions with participant. Staff must be able to review a participant's and/or a family's enrollment, benefits and premium history and then enter data into a Call Tracking system to create a 'tickler' for call back and follow up of calls. Access to routine information on the Internet is accomplished through the pool website. The website includes provider directories and provider look up through a link to its claim administrator and a description of eligibility and benefits through a series of questions that direct the person to the pool plan descriptions. In an effort to ensure quality customer service is maintained, the following functionality should be included with any software solution selected

A future consideration for claim processing is for the new system to allow staff to classify claims for manual adjudication even though they may have been set up for auto-adjudication. Staff must be able to automatically release pended claims with no staff review or after audit review. If the automated claims audit program finds a problem with a claim that it cannot resolve staff must be able to put the claim on system hold for staff to process. The system must allow staff to find pended claims, to review the claim document and data screens side-by-side and make the decisions necessary to adjudicate the claim. The system must automatically audit all claims in a uniform, consistent basis.

Individual Insurance Policyholders will be able to do anything that members can do. For individual insurance, members are family members of the policyholder. For group insurance, policyholders and employers are synonymous whereas members and employees also mean the same. For reinsurance, policyholders are the carriers that reinsure with the pool. No members can use the systems for reinsurance.

	FUNCTIONAL REQUIREMENTS
A1	General Requirements
A1.1	Fully audited Premium billing and accounting
A1.2	Support maintenance and processing of all billing files
A1.3	Setup and maintenance of group/individual rate files
A1.4	Manual billing adjustments
A1.5	Premium reconciliation
A1.6	User-designed statement formats
A1.7	Billing comments entry
A1.8	Automatic (retroactive) adjustments
A1.9	Support for billing and reporting
A1.10	Capability to prioritize cash postings to billed items
A1.11	Flexible, user-defined billing formats
A1.12	Billing statement generation, print, and reprint
A1.13	Billing updates integrated with claims and eligibility
A1.14	Creation of premium invoices

	FUNCTIONAL REQUIREMENTS
A1	General Requirements (Cont.'d)
A1.1	Built in tickler system for member related issues
A1.2	Member verification
A1.3	Free-form comments (through role-based security)
A1.4	Routing capability
A1.5	Tickler capability (issue and task reminders)
A1.6	Supervisor management functionality
A1.7	Work distribution management
A1.8	Performance tracking
A1.9	Automatic adjustment of billing information due to changes to eligibility
A1.10	Ability to process global rate adjustments
A1.11	The software should not be vendor hardware specific, in other words if the software is server based, it should be able to operate on a generic group of servers, not one particular vendor's server
A1.12	Electronic Data Interchange (EDI) capability is required, with a preference for utilizing the HIPAA standard transactions and code sets
A1.13	If the system is EDI capable but the software requires a translator to be used, a description of plans to move to standard code sets must be provided
A1.14	Electronic Data Interchange (EDI) capability is required, with a preference for utilizing the HIPAA standard transactions and code sets
A1.15	The system should be a real-time benefit administration system
A1.16	It should have a full range of functionality for eligibility, customer service, billing, and collections and be capable of automated interface with a fully functional claims administration system

	FUNCTIONAL REQUIREMENTS
A1	General Requirements (Cont.'d)
A1.1	The presentation layer should be browser based rather than windows based or text-driven
A1.2	Data entry screens must be capable of customization.
A1.3	Integrate the system with desktop office productivity software.
A1.4	Provide mail-merge capabilities
A1.5	Ad hoc reporting capabilities, preferably with supplied canned reports, with the capabilities to modify and create additional reports as needed from a standard report writing software package such as Crystal Reports
	Input capabilities via:
A1.5.1	OCR
A1.5.2	IVR
A1.5.3	Paper
A1.5.4	Web
B1.1	PAI conducts enrollment (834) functions this may require PAI to send Trading Partners an electronic 834 transaction. Likewise, for reinsurance, carriers that are Covered Entities may notify PAI of their intent to cede an individual or a whole group with the same 834 transaction or they may send notification in the current non-standard format
B1.2	PAI verifies eligibility (270/271); primarily notifying the carriers that premium has been received. This will require PAI to send a standard transaction
B1.3	PAI may be required by the carriers to receive a full claims transaction (837). The current claims transactions sent by carriers are not full 837 transactions. Carriers that are Covered Entities that can dictate that their Business Associate receive a full 837 transaction and PAI's only alternatives would be to either accept the full transaction or to deny it and limit the carrier's participation in the pool.
B1.4	Full audit capabilities to do accounting for disclosure must be provided, including tracking of both authorized and unauthorized access to personal health information (Logging of the access at the application level rather than the database level).
B1.5	There must be role based security components to restrict access to information on a "need to know" basis with a stringent security template to track usage. Password protection and encryption capabilities for all transactions must be provided.

	FUNCTIONAL REQUIREMENTS
	HIPAA Requirements (Cont.'d)
B1.6	Compliant with HIPAA standards with respect to National Provider Identifier (NPI)
B1.7	Compliant with HIPAA standards with respect to National Employer Identifier Number (EIN)
B1.8	Compliant with HIPAA standards with respect to the following:
B1.8.1	Individual authentication of users
B1.8.2	Access controls
B1.8.3	Audit trails
B1.8.4	Physical security and disaster recovery
B1.8.5	Protection of remote access points