HIMSS Healthcare Information and Management Systems Society

PHOENIX HEALTH SYSTEMS

U.S. Healthcare Industry HIPAA Compliance Survey Results: Summer 2004

U.S. Healthcare Industry HIPAA Survey Results: Summer 2004

Executive Overview

Phoenix Health Systems and HIMSS have sponsored the quarterly U.S. Healthcare Industry HIPAA Survey since the beginning of 2000. As of 2004, the survey is being conducted semi-annually. Therefore, the Summer 2004 Survey follows the last published results from January of 2004. The findings reflect the industry's compliance status with the HIPAA regulations at this time when the deadlines for Privacy and Transactions / Code Sets have passed and as the Security effective date rapidly approaches in April of 2005.

As we continue to move toward compliance with all aspects of the HIPAA regulations, it is clear that the road has been rocky and full of both expected and unpredicted challenges. Clearly, the industry has made great progress over the past four years in its goal to achieve compliance and operationalize the HIPAA requirements, but the responses to the Summer 2004 Survey indicate that there is still much work to do.

In general, relatively complete Privacy compliance by all or most covered entities does appear to be on the horizon. Hopefully, the experience of having addressed the cultural, administrative and systems-related complexities of deploying HIPAA Privacy programs will result in a more effective and rapid implementation of the Security Rule. But, it is in the area of Transactions and Code Sets (TCS) standardization that the industry continues to have the greatest difficulties in achieving compliance. Many organizations have not yet implemented those transactions required for their business functions, while others that are compliant are negatively affected by their non-compliant trading partners. Although progress is being made, the industry is not even close to realizing the promise of a return on investment from the standardization of our healthcare business transactions – despite having passed the compliance deadline last October 16 – more than nine months ago!

It will be interesting to see where covered entities will be in six months, when we conduct the next survey. Will most organizations finally be compliant with ALL of the transaction requirements or will we still have a Centers for Medicare and Medicaid Services (CMS) Contingency Plan in place? One would expect that, by that time, Privacy compliance will no longer be an implementation goal and will exist, rather, as a state of mind for all covered entities. And, in six months time, we will also be counting the days for the Security compliance deadline. Across-the-board HIPAA compliance is definitely coming, but the question remains – WHEN?

Key findings of the Summer 2004 Survey include:

- **HIPAA Transactions and Code Sets**
  - ✓ Progress with TCS compliance is not overly encouraging – only 65% of Providers, 62% of Payers, and 64% of Clearinghouses indicated that they are currently fully compliant.
  - ✓ Less than half of Providers and Payers are conducting all of the standard transactions required for their business functions.
  - ✓ Of the covered entities not yet compliant, 68% have completed internal testing, but only 27% have completed external testing. Only 50% of Providers and 46% of Payers have completed other TCS remediation activities not related to testing.
  - ✓ Half (50%) of Providers and 63% of Payers indicated that there are transactions which their information systems are *capable* of producing, but that are not being conducted due to the inability of their trading partners to accept/transmit them.

- ✓ When asked the reason for their lack of full TCS compliance, most covered entities cited their trading partners' lack of compliance and coordination as causes.
- ✓ Approximately 40% of Providers, 36% of Payers, and 51% of Vendors feel that CMS should maintain its Contingency Plan for at least another three months.

- **HIPAA Privacy**
  - ✓ Twenty-two percent (22%) of Providers and 9% of Payers reported that they remain non-compliant with the Privacy Rule, more than a year after its effective date (April 2003).
  - ✓ Even among "compliant" organizations, gaps remain in certain areas, such as establishing Business Associate Agreements and monitoring internal Privacy compliance.
  - ✓ Sixty-four percent (64%) of Provider and 58% of Payer respondents reported their organizations had experienced between one and five privacy breaches in the first six months of 2004.

- **HIPAA Security**
  - ✓ Initiatives for Security Rule compliance are moving slowly – across the industry, the majority of respondents reported their organizations will not be fully compliant until 2005.
  - ✓ Providers (87%), Payers (91%), and Clearinghouses (90%) indicated they will be compliant on or before the deadline.
  - ✓ Thirty-one percent (31%) of total Providers, Payers and Clearinghouses responded that their organizations had experienced at least one data security breach in the first six months of 2004.

THE SURVEY

Phoenix Health Systems and HIMSS conducted the Summer 2004 U.S. Healthcare Industry HIPAA Compliance Survey from June 1 to June 15, 2004. A total of 540 healthcare industry representatives responded to e-mail invitations to participate in the survey that were sent to HIMSS 13,000+ members and to Phoenix' 19,000+ HIPAAlert newsletter subscribers. The online survey was anonymously completed via the Phoenix' web site, HIPAAdvisory.com.

The Participants

Eighty-six percent (86%) of total survey respondents hold an "official" role within their organization for HIPAA compliance. More than half of respondents (57%) are CIOs, senior managers, and department managers, and 29% work specifically in the compliance/security area. Provider organizations accounted for 73% (393) of participants. The distribution of survey participants follows:

- Providers – 73%
  - ✓ Hospitals with 400+ beds: 21%
  - ✓ Hospitals with 100-400 beds: 16%
  - ✓ Hospitals with less than 100 beds: 14%
  - ✓ Medium-sized physician practices (11 to 29 physicians)/other providers: 7%
  - ✓ Small physicians practices (10 or fewer physicians)/other providers: 15%
- Clearinghouses – 3%
- Payers – 14%
  - ✓ Covering fewer than 150,000 Lives: 5%
  - ✓ Covering 150,000-500,000 Lives: 3%
  - ✓ Covering 501,000-1,500,000 Lives: 3%
  - ✓ Covering more than 1,500,000 Lives: 3%
- Vendors – 10%
  - ✓ Annual Revenues less than $50M: 7%
  - ✓ Annual Revenues of $50M-$100M: 1%
  - ✓ Annual Revenues more than $100M: 2%

(**Note:** Throughout this report, the very small sample size of Clearinghouse respondents should be considered in conclusions provided for this group.)

CONSIDERING INTEROPERABILITY BETWEEN HIPAA STANDARDS

A new topic examined in the Summer 2004 Survey was the inter-relationship among the requirements of the HIPAA Privacy, Security, and TCS regulations. Within the three separate HIPAA rules, there are some requirements that conflict and others that need coordination between similar standards in the different rules – this is what is meant by "interoperability." Half of both groups – Providers (50%) and Payers (51%) – have established mechanisms to analyze this interoperability. Of those respondents, the overwhelming majority (almost 100%) use a HIPAA Steering Committee, in addition to other established working groups intended to oversee all HIPAA-related activities. More than half also indicated they have designated individuals within their organizations assigned to this task.

We asked participants specifically about those individuals within their organizations appointed as the Security Official and the Privacy Official. Eighty-seven percent (87%) of Providers, 89% of Payers, and 100% of Clearinghouse organizations had appointed a Security Official as of June 2004. Of those respondents whose organizations had appointed Security Officials, 39% of Providers, 40% of Payers, and 80% of Clearinghouses indicated their Security Official also holds the title of Privacy Official.

TRANSACTIONS AND CODE SETS COMPLIANCE

The official deadline for compliance with the HIPAA Transactions and Code Sets regulations was October 16, 2003 – more than nine months ago. Due to industry-wide difficulties in achieving TCS compliance, CMS implemented a temporary Contingency Plan on September 23, 2003 that allowed covered entities to continue to transmit non-compliant transactions. Many Payer organizations offered similar contingency plans. When this survey was conducted in early June, the CMS plan was still in effect. In light of the fact that many covered entities still operated according to the original CMS Contingency Plan, the Summer 2004 Survey examined TCS compliance issues and implementation progress. (Note: Since the completion of the survey, CMS has announced a modification to the Contingency Plan. Although the plan is still in effect, any non-compliant claims submitted to Medicare will require an extra thirteen days to process.)

Overall TCS Compliance

Compliance with the TCS regulations includes implementation of all necessary policies, procedures, processes and systems in order to first test and then regularly conduct the standard HIPAA transactions required for the business functions performed by the covered entity.

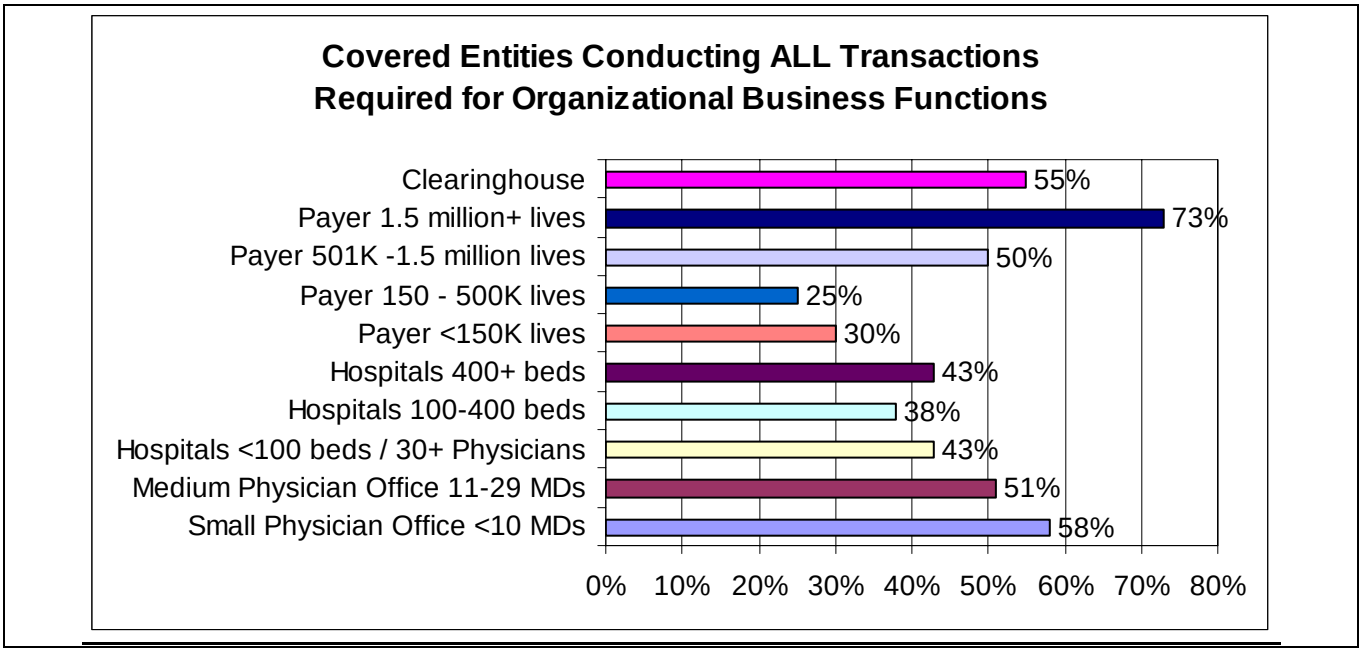
The overall results for responses to questions about TCS compliance are not very encouraging. Only 65% of Providers, 62% of Payers, and 64% of Clearinghouses indicated that they are currently fully compliant with the TCS rule. Most (89%) of the remaining "non-compliant" organizations have completed a gap analysis, but only 50% of the Providers and 46% of the Payers have completed TCS remediation activities other than transactions testing.

A large percentage of covered entities (Payers, Providers, and Clearinghouses) responding to the survey who are **not** yet compliant with the TCS regulations are still in the testing phase, with 68% having completed internal testing, but only 27% having completed external testing. Seventy-three percent (73%) of non-compliant Payer respondents have completed internal testing, but only 9% of them have completed external testing. In contrast, while 65% of non-compliant Provider respondents have completed internal testing, 29% of the same group has completed their external testing plans.

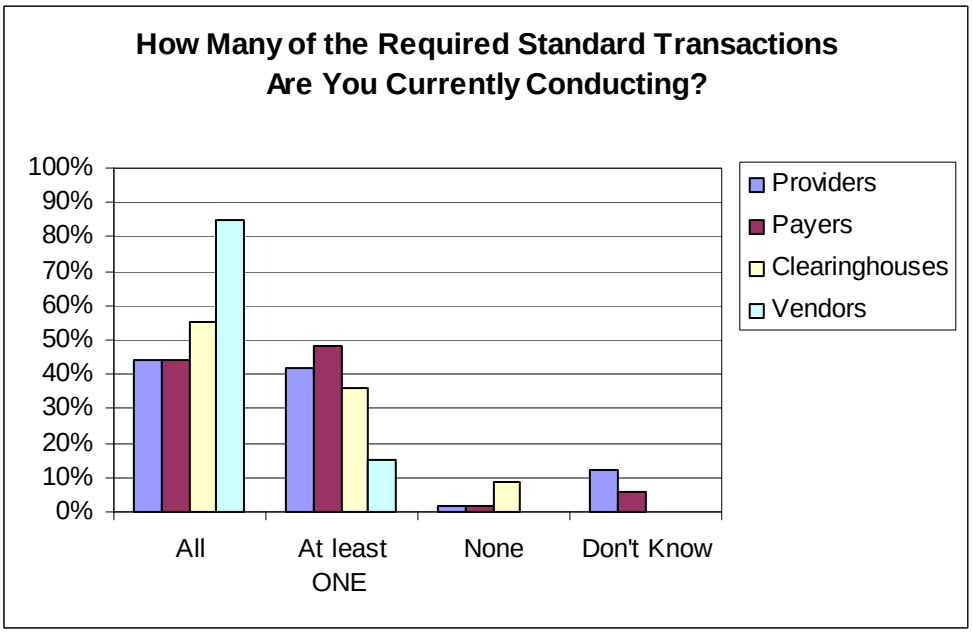
Readiness to Accept/Transmit HIPAA Transactions

The key measure of TCS compliance focuses on whether a covered entity is currently conducting the transactions required for its business functions *using the standard HIPAA transactions.* To assess the industry's adherence to using standard transactions, respondents were asked to: "Indicate your

organization's current status relative to electronically conducting the standard HIPAA transactions required for business functions performed by your organization." Responses to the survey indicated that less than half of the participants are actually compliant with respect to *using* the standard transactions. Only 44% of the total Provider respondents and 44% of the total Payer respondents were conducting all of the transactions required for their specific organizations. The chart below summarizes the "compliance" of the different respondent groups in terms of conducting the required transactions.



If an average of less than half of the industry is conducting ALL of the transactions that HIPAA requires of them, then the question is "what is the other half doing"? It appears that those not conducting all of their required transactions are at least making some progress toward full compliance. Approximately half (42% of Providers and 48% of Payers) indicated they are conducting "at least ONE but NOT ALL" of the transactions required for their business functions (as shown in the graph below). If there is a positive note in this overall lack of *full* compliance with the TCS regulations, it is that only 2% of both the Provider and Payer respondents indicated that they were conducting "NONE" of the standard transactions.



An interesting related note is that, when asked if they were fully compliant with the TCS requirements, 65% of the Providers indicated they were fully compliant, but when asked if they were conducting the necessary standard transactions for their organizations, only 44% responded that they were doing so. A similar pattern existed within the Payer group, where 62% of respondents reported "full compliance" but only 44% indicated they were conducting all of their required transactions. When the data was further analyzed regarding the actual transactions being conducted, it became apparent that participants viewed being "ready to conduct" or "capable of conducting" as being compliant – as opposed to actual implementation of all required transactions.

When participants were asked if there were transactions that were *not* being exchanged with their trading partners even though their own information systems were capable of conducting them, 50% of Providers and 63% of Payers said "Yes." Of those, 51% of Providers reported the actual reason was that their Payers were not ready to accept/transmit those transactions, and 34% of Providers indicated their Clearinghouses were not ready. Sixty-two percent (62%) of Payers claimed their systems were capable of conducting certain transactions that their Providers could not yet process. (See additional comments under "Roadblocks to HIPAA Compliance" below.)

Both Providers and Payers expressed moderate confidence that Vendors are capable of supporting needed HIPAA-compliant standard transactions. Among Providers, 57% are either already using their vendor's software for ALL their required transactions, or have confirmed that the software is capable of conducting them. Sixty-seven percent (67%) of Payers confirmed that their vendor-supplied applications are able to transact all HIPAA standard transactions/code sets. The majority of Payer organizations (81%) use vendor software applications for some portion of their standard transactions processing, and 86% of them indicated their Vendors have provided updated versions to support HIPAA compliance.

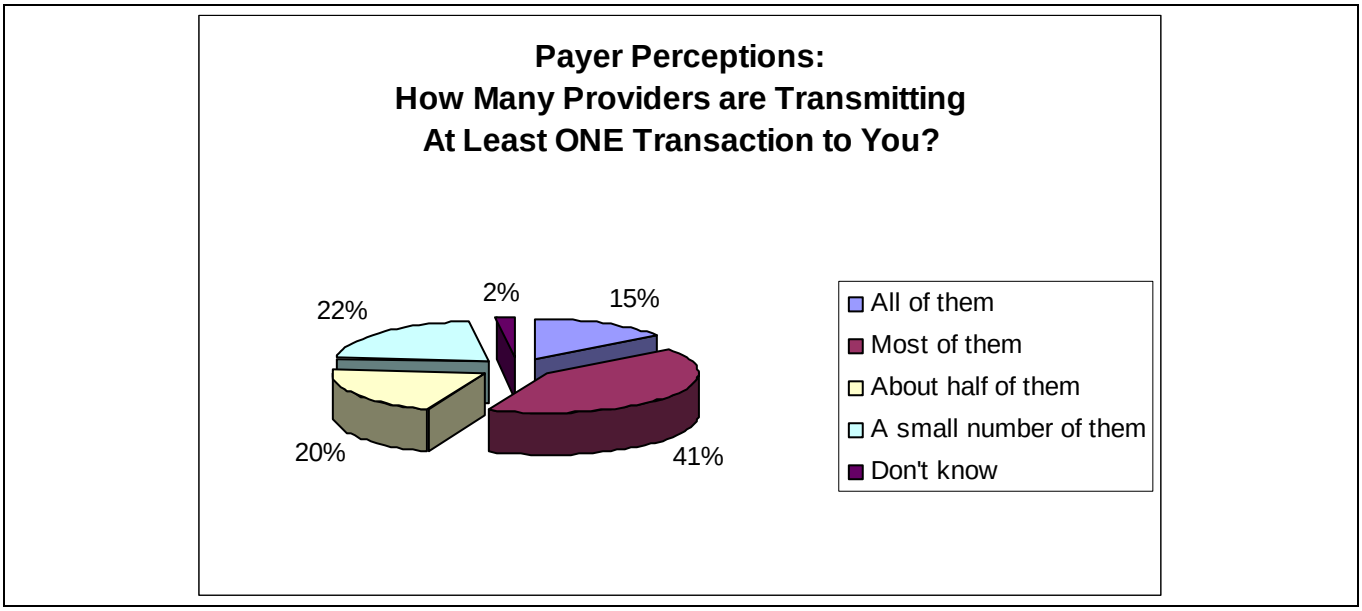
Confidence in their Clearinghouses' ability to produce the standard transactions varied among the survey participants. Clearinghouses were expected to be the answer for many covered entities that chose not to remediate their software applications for full TCS compliance. It appears, however, that this solution has yet to be put into universal practice. Participants were asked: "How do you perceive your Clearinghouse(s) readiness to transact all HIPAA standard transactions required for your business functions?" The following chart provides a summary of the primary responses, and indicates the extent to which Providers and Payers are successfully using Clearinghouses to conduct standard transactions with their trading partners.

Perception of Capability of Clearinghouses To Produce ALL of the Required Standard Transactions

	Providers	Payers
Our organization is currently conducting ALL HIPAA standard transactions required with our Clearinghouse(s)	**51%**	**41%**
Our organization is currently conducting ONE OR MORE BUT NOT ALL standard transactions required with our Clearinghouse(s)	**30%**	**31%**
Clearinghouse(s) currently ready to transact ALL HIPAA standard transactions required, but our organization has not yet begun to conduct the transactions	**2%**	**3%**
Clearinghouse(s) currently ready to transact ONE OR MORE BUT NOT ALL HIPAA standard transactions, but our organization has not yet begun to conduct the transactions	**3%**	**9%**

Since many covered entities are not yet conducting ALL of the required standard transactions, their Clearinghouse(s) may be satisfying their current needs. However, according to survey participants, their Clearinghouse(s) still lacked the capability to conduct ALL of the transactions.

The majority of Providers (67%) perceived their Payers to be capable of handling the required transactions. Although 87% of Payers reported that they currently accept HIPAA standard transactions from Provider clients, either directly or through a Clearinghouse, their perception of the overall success of Provider clients in implementing the standard transactions is not particularly positive. We asked those same Payers: "How many of your Provider trading partners are transmitting AT LEAST ONE of the HIPAA standard transactions to you (either directly or through a Clearinghouse)?" Their responses are displayed in the chart below, indicating that only 15% of the Payers reported that ALL of their Provider clients were conducting at least one transaction, and only 41% said that MOST of their clients were doing so.



Sixty-two percent (62%) of Vendors indicated that ALL of their clients are using their software applications to conduct at least ONE but NOT ALL the transactions required for organizational business functions. However, the Vendor respondents indicated that only 39% of their clients were conducting ALL of the necessary HIPAA standard transactions.

Although the industry is moving forward in its implementation of the transactions, it is important to note that the TCS regulations required that ALL standard transactions be put into place last October. For many, the CMS Contingency Plan has obviously been necessary. On a more positive note, CMS has reported that 93% of the claims submitted to Medicare for the period June 28 - July 3, 2004 were HIPAA compliant – but it must be noted that this statistic measures only the 837 transaction. The question to be answered is "WHEN will the industry as a whole be conducting ALL the standard transactions and be able to state that TCS compliance has been accomplished?"

Transactions Currently Being Conducted

Although many covered entities have yet to implement ALL of the standard transactions, WHICH transactions are they currently conducting? For respondents who stated they are conducting at least ONE but NOT ALL of the standard transactions, the chart below displays the transactions they ARE conducting. As would be expected, these covered entities are primarily focused on the 837 (Claims), and to a lesser degree the 835 (Payment/Remittance Advice).

Standard Transactions	Provider	Payer	Clearinghouse
837 Claims, COB, Equivalent Encounter	77%	90%	75%
835 Payment, Remittance Advice	51%	50%	75%
276/277 Claims Status	17%	47%	50%
270/271 Eligibility for Health Plan	24%	47%	75%
834 Enrollment/Disenrollment	12%	47%	0%
820 Premium Payment	12%	23%	0%

It is apparent that universal implementation of the TCS standard transactions is NOT imminent. Only 21% of Providers and 33% of Payer participants in the survey expect to be ready within the next 3 months to conduct ALL of the transactions needed for their business functions – which raises the issue of how long the existing contingency plans by CMS and other payers will continue.

CMS' Temporary Contingency Plan

CMS announced a contingency plan on September 23, 2003, in response to the industry's inability to comply with the October 16, 2003 TCS deadline. Many organizations have taken advantage of the CMS plan to allow continued processing of non-compliant Medicare claims and similar contingency arrangements implemented by other health plans.

When asked how the CMS Contingency Plan announcement had impacted their overall TCS course of action, about one-third of both the Provider and Payer respondents replied they had altered their implementation plan and continued to accept non-compliant transactions. Over half (52%) of Providers and 42% of Payers indicated that the Contingency Plan had no effect on their action plans because they were "already compliant." In offering its Contingency Plan, CMS stated that demonstration of "good faith efforts" toward eventual TCS compliance was expected for all who chose to use the plan. The majority of Providers (93%) indicated they were confident in their abilities to demonstrate such efforts if requested.

On July 1, CMS announced a modification to the Contingency Plan (non-compliant claims submitted to Medicare will require an extra 13 days to process), but indicated that the overall plan is to remain in effect. Prior to this announcement, we asked Providers, Payers and Vendors to specify how long they felt CMS should maintain the Contingency Plan – 40% of Providers, 36% of Payers, and 51% of Vendors indicated that CMS should maintain it for up to three months. A substantial number (35% of Providers, 39% of Payers, and 22% of Vendors) wanted the plan to be extended four to six months or longer.

Identifying the Obstacles to TCS Implementation

The big issue of WHY the industry has been unable to achieve TCS compliance involves a fair amount of "finger pointing." When survey participants were asked to select the "reasons" for the lack of compliance, they responded (in ranked order) as follows:

- **Providers**
  - ✓ Payers are not ready to accept standard transactions.
  - ✓ Clearinghouses are not ready to accept or transmit transactions.
  - ✓ There are ambiguities in information released by CMS regarding transaction requirements.

- **Payers**
  - ✓ Providers are not ready to accept standard transactions.
  - ✓ There are ambiguities in information released by CMS regarding transaction requirements.
  - ✓ Clearinghouses are not ready to accept or transmit transactions.

- **Clearinghouses**
  - ✓ Payers are not ready to accept/transmit standard transactions.
  - ✓ Providers have not captured the data required for the standard transactions.
  - ✓ There are ambiguities in information released by CMS regarding transaction requirements.

- **Vendors**
  - ✓ Payers are not ready to accept/transmit standard transactions.
  - ✓ There are ambiguities in information released by CMS regarding transaction requirements.
  - ✓ Providers have not captured the data required for the standard transactions.

Sample of Respondents' Comments/Responses

Provider: "Payers are not ready to return 835s in standard format. This includes governmental payers as well as private payers. Providers were required to meet the timeframe for 837 submission, but payers are slow and difficult to work with in getting the remittance returned in a timely manner."

Provider: "While significant progress has been made in 837 compliance, trading partners not willing or currently unable to provide other transactions that would be of great benefit to the provider market (835)."

Payer: "Vendors of the Providers are not ready to test/send compliant transactions to us; TPAs of employers are not willing to send compliant 834 transactions to us."

Vendor: "Many payers are requiring providers to report information beyond that specified in the HIPAA Implementation Guides thus resulting in non-standard transaction code sets. We're heading back to the same situation of non-standard files."

Payer: "Working with Clearinghouses has been a challenge; they blame lack of compliant data on providers."

In addition to readiness issues, third party communication remains a problem. Respondents continue to assert that their own organizations have been cooperative and forthcoming with information, and blame business partners for poor communications. Payers (90%), Clearinghouses (100%), and Vendors (96%) said they had communicated "all" or "much" information to their clients regarding HIPAA compliance plans, progress, and timelines. Only 73% of Providers and 69% of Payers identified Clearinghouses as "moderately" to "very" forthcoming. Only 73% of Providers and 75% of Payers considered Vendors to be "moderately" to "very forthcoming."

When asked if they had provided assistance to their Providers in efforts toward HIPAA compliance, 77% of Payers said they had provided "much" or "moderate" support. However, only 47% of Providers felt that their Payers had provided them with a satisfactory level of needed assistance. In addition, only 58% of Providers considered Payers to be forthcoming with required information. Obviously, there is a disagreement among the various groups about the cooperation of their trading partners in the TCS compliance effort.

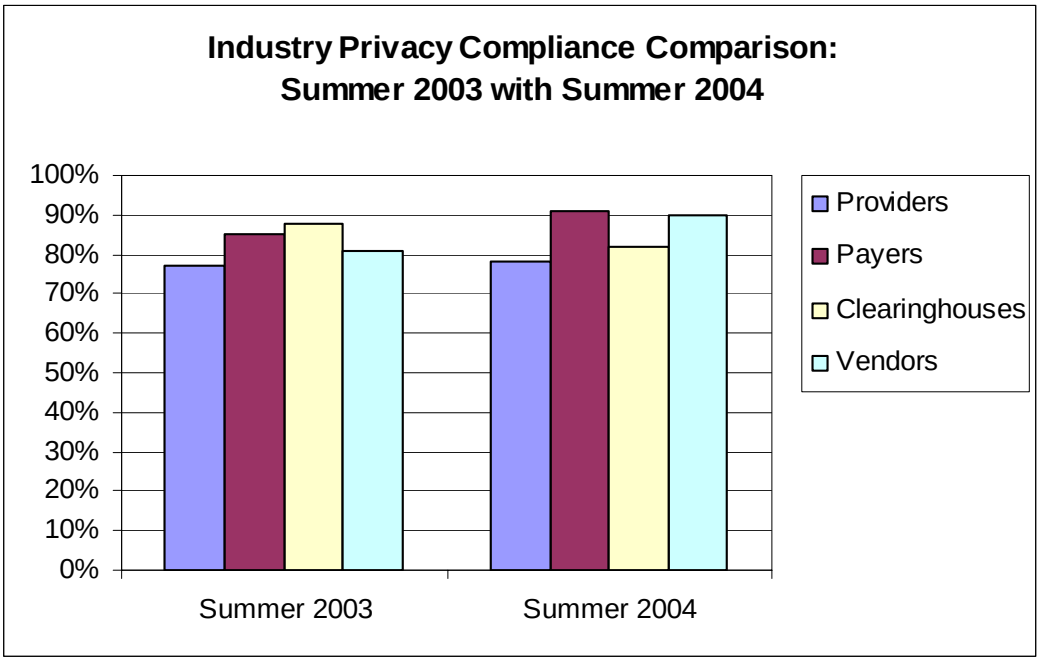
The Administrative Simplification Enforcement Tool (ASET)

Given the frustration widely expressed by covered entities concerning the cooperation and readiness of their trading partners, we asked survey participants whether they had availed themselves of ASET – a support tool provided by the Office of HIPAA Standards to allow covered entities and others to submit complaints against entities whose actions impact the ability of a transaction to be accepted and/or efficiently processed.

Only 35% of Providers and 38% of Payers indicated awareness of the availability of ASET. Only 10% of Providers and 4% of Payers reported they had used ASET to register a complaint. Nine percent (9%) of Providers and 2% of Payers reported that they had been the subject of a complaint registered through ASET.

PRIVACY COMPLIANCE

Compliance with the HIPAA Privacy Rule was required by April 2003. This survey has continued to track the healthcare industry's Privacy compliance progress to identify any remaining compliance gaps. Ninety-one percent (91%) of Payer respondents indicated they were now compliant with the HIPAA Privacy regulations. (In the January survey, 86% of Payers had indicated that they were compliant with the Privacy regulations.) Providers continue to lag behind with only 78% (down from 80% during the last survey) reporting their organizations were in full compliance.



Within the group of respondents from the Provider sector, medium-sized physician practices were the "most compliant" (94%), while hospitals with 100 - 400 beds were the "least compliant" (67%).

As in past surveys, Privacy "compliant" organizations were asked to clarify whether gaps remained between their actual privacy practices and the requirements of the Privacy standards. (See table below.) Responses to questions about specific Provider privacy practices indicate that they have been diligent in addressing the regulations. Provider compliance in this area has improved since the last survey, especially in the area of "monitoring organizational compliance with the Privacy Regulations" – up from 76% in the January survey to 85% this survey. Providers also improved in the area of required Business Associate Agreements – up from 73% to 80% – although this remains the area of greatest non-compliance. Eighty-one percent (81%) of Vendors (which are not covered entities but are key players in the establishment of Business Associate relationships) replied that they have all required Business Associate Agreements in place with their clients (down from the last survey in which Vendors indicated a compliance level of 85%).

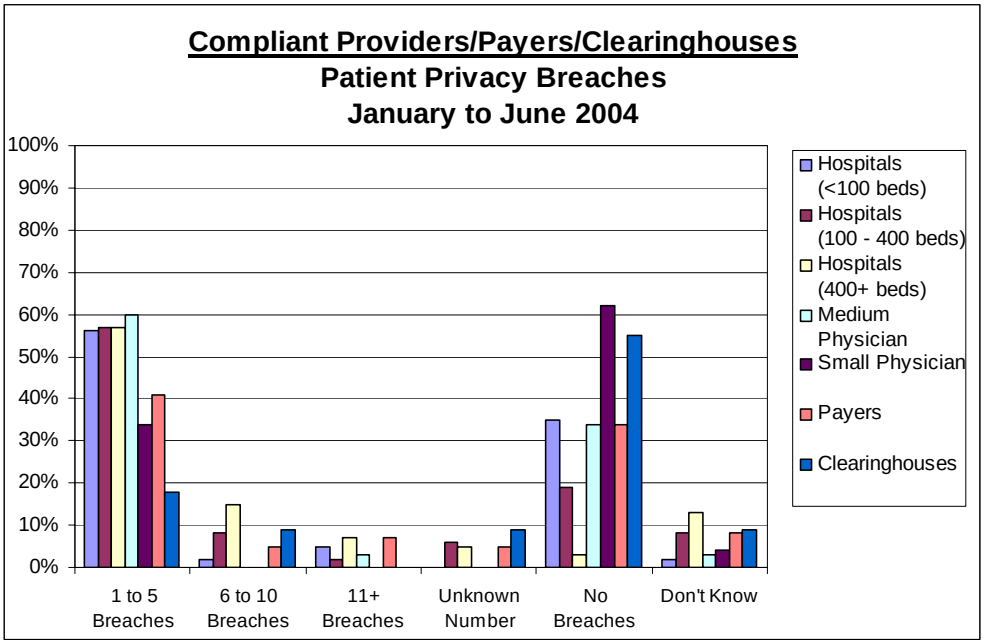
Summary of Privacy Practices Implemented for "Compliant" Organizations		
Areas of Privacy Compliance:	**Providers**	**Payers**
Obtain Patient Authorizations for use and disclosure of PHI	**100%**	**95%**
Obtain acknowledgement of receipt of Notice of Privacy Practices	**99%**	**N/A**
Enable mandated patients' rights (review, amend, restrict records)	**98%**	**97%**
Post and distribute Notice of Privacy Practices	**98%**	**93%**
Maintain Accounting of Disclosures	**97%**	**93%**
Provide ongoing Privacy training	**97%**	**97%**
Use "Minimum Necessary" Restrictions	**95%**	**N/A**
Document Privacy policies and practices	**95%**	**95%**
Implement security protections as required under the Privacy Rule	**91%**	**90%**
Provide overall workforce Privacy training updates	**91%**	**88%**
Monitor organizational compliance with Privacy regulations	**85%**	**83%**
Have obtained all required Business Associate Agreements	**80%**	**90%**

When Providers and Payers were asked which areas of privacy compliance presented the greatest challenge, they ranked "managing the organizational process for accounting of disclosures" as the number one challenge and "maintaining 'minimum necessary' when handling requests for disclosure of PHI from third parties" as the second most challenging.

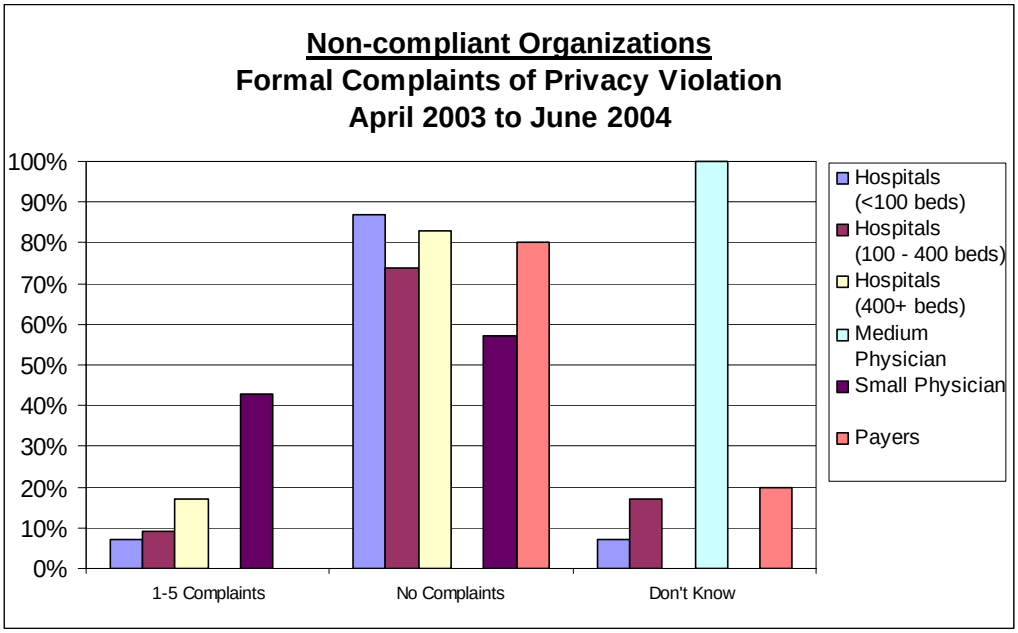
The majority of respondents who indicated that they are **not** yet compliant with the Privacy regulations have completed a Privacy gap analysis – 79% of Providers and 80% of Payers. Privacy training has been completed by 92% of larger hospitals that are not yet compliant, but only 40% of smaller hospitals have reached this milestone. On a more positive note, 71% of non-compliant Providers expect to complete Privacy remediation within the next three months.

Incidents of Patient Privacy Breaches

The Summer 2004 Survey questioned "compliant" participants about reported incidents of patient privacy breaches from January to June of 2004. Almost two-thirds (64%) of Providers and over one-half (58%) of Payers reported occurrences of privacy breaches. For Provider respondents: 52% indicated that they had 1-5 privacy breaches, 6% had 6-10 breaches and 3% had 11 or more breaches. (See table below.)

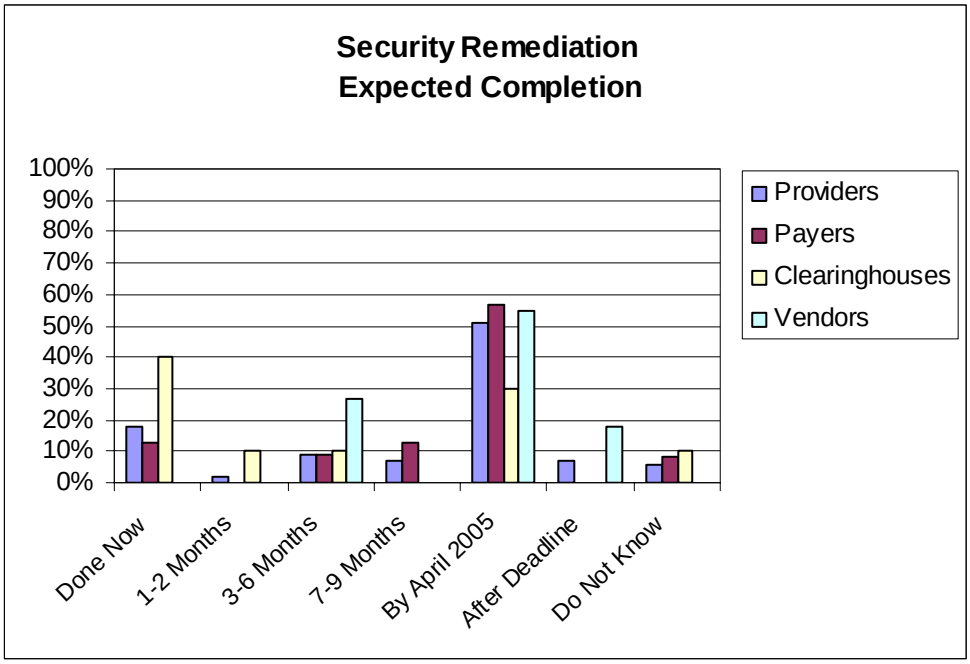


As might be expected, a higher percentage of non-compliant organizations (72% of Providers and 80% of Payers) had occurrences of Privacy breaches than compliant organizations over the last six months. We also asked non-compliant organizations if they had had any formal Complaints of Privacy Violation (either Federal or in a civil proceeding) since the Privacy deadline in April 2003. Seventy-six percent (76%) of non-compliant Providers and 80% of non-compliant Payers had no formal complaints filed against them.



SECURITY COMPLIANCE

Although compliance with the Security Rule is not required until April 2005, we asked all industry groups to indicate current levels of compliance, projected timelines for remediation efforts (see table below) and measures implemented to ensure secure transmission of transactions. Organizations appear to be focusing on Security at this time, but progress toward compliance remains slow. Providers did make some progress over the past six months, with compliance levels increasing from 12% in the Winter 2004 Survey to 18% in the Summer 2004 Survey. However, compliance levels among Payers (13%) and Clearinghouses (40%) have not improved since the last survey. Sixty-five percent (65%) of Vendors feel they are meeting their Security Rule-related obligations today as a Business Associate of covered entities. The majority of all groups expect to achieve compliance by April 2005 – Providers (87%), Payers (91%), Clearinghouses (90%), and Vendors (82%) say they will be ready on or before the deadline.



As we count down to the Security compliance date, organizations not yet compliant with the Security regulations plan a focused commitment to security remediation. Providers (45%) and Payers (43%) indicated that they plan to complete organizational security training within the next six months, and the vast majority (95%) plan to be finished by the deadline in April 2005. Full implementation of organizational security policies and procedures will take longer for most organizations – only 32% of Providers and 37% of Payers plan to complete this implementation by the end of 2004. However, 92% of Providers and 95% of Payers do report expected completion by the Security compliance deadline.

Required HIPAA Security Standards – Most Difficult to Implement…

Providers and Payers differed only slightly in their assessment of which HIPAA Security standards were most difficult to implement. The responses below are ranked in descending order of the percent of respondents who cited the standard. (Note: respondents were asked to indicate ALL of the standards they found difficult to implement – therefore, figures below reflect the percentage of each group who checked off the noted item as ONE of the standards they found difficult to implement.)

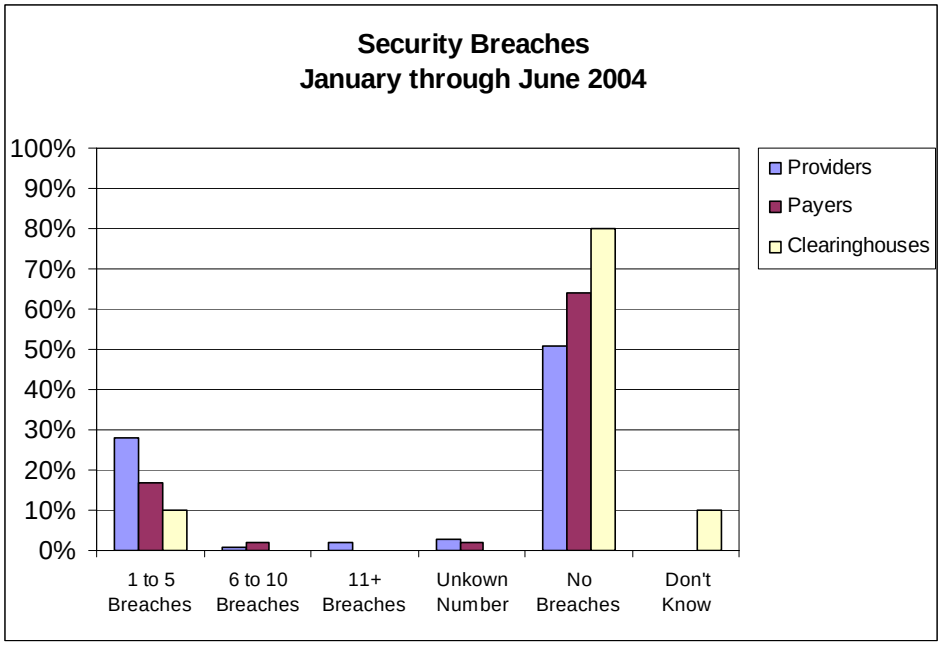
- **Providers**
  - ✓ Audit Controls (52%)
  - ✓ Risk Management/Risk Analysis (48%)
  - ✓ Information System Activity Review (39%)
  - ✓ Data Backup Plan/Disaster Recovery Plan/Emergency Mode Operation Plan (34%)

- **Payers**
  - ✓ Risk Management/Risk Analysis (36%)
  - ✓ Information System Activity Review (30%)
  - ✓ Data Backup Plan/Disaster Recovery Plan/Emergency Mode Operation Plan (26%)
  - ✓ Audit Controls (23%)

Incidents of Data Security Breaches

Providers, Payers, and Clearinghouses were asked to indicate the number of security breaches their organizations had experienced since January 2004. Over 30% of the group had experienced at least one data security breach, with 28% of Providers (up from 21% in Winter 2004) and 17% of Payers (down from 25%) reporting that they had experienced one to five data security breaches. See full

results on this question in the table below. (Note: since compliance with the Security regulations is not yet required, it is likely that some organizations have yet to fully establish tracking mechanisms for security breaches.)



Are You Transmitting Secure Transactions?

Because covered entities were required to implement HIPAA standard transactions long before Security Rule compliance was required, a justifiable concern is whether the transactions could be considered secure. We solicited comments on the following question: "How is your organization ensuring that it will be transmitting secure (PHI-protected) compliant transactions if you have not completed your security remediation efforts?" The following list indicates the solutions most frequently reported:

- ✓ Virtual Private Network (VPN)
- ✓ Encryption
- ✓ Secured Socket Layer (SSL) Web Site
- ✓ Direct Connection to Third Party
- ✓ Bulletin Board System (BBS) Connection
- ✓ Secure Dedicated Lines
- ✓ Password Protection
- ✓ Secure File Transfer Protocol (FTP)
- ✓ Authentication and Access Control on Transactions
- ✓ Strict Policies and Procedures

In response to the question noted above, many respondents reported the use of sound measures to secure transactions. However, as shown in the comments from Payers and Providers below, there is reason for concern about secure transmission of transactions in some organizations.

- "We are awaiting installation of new EMR system before fine tuning our security rules/measures. For the present we believe we are compliant."
- "Only through policy."
- "We are using a variety of tools where possible. Where not, we are applying the minimum necessary rule."
- "We are not."

- "Relying on vendor/clearinghouse and payer software."
- "We will be compliant by 01/01/05."
- "We will do a risk analysis and go from there."
- "We have audited that area in the past."
- "This is not a requirement of the security rule."

ROADBLOCKS TO HIPAA COMPLIANCE

As we continue to track "major roadblocks" to overall HIPAA compliance across the industry, we are seeing a shift in emphasis away from broad issues such as budget and time constraints (which ranked third and fourth respectively in the Summer 2004 Survey) to issues more specific to day-to-day operations. "Achieving successful integration of new systems, policies, and procedures across the enterprise" ranked as the primary impediment to HIPAA compliance in this survey, up from second place in January 2004. "Interpretation of HIPAA Regulations" ranked second in this reporting period (down from its number one position in the January 2004 survey), and written comments support the contention that varying interpretations of the HIPAA regulations is a major concern.

Sample of Written Survey Comments/Responses

Payer: "Multiple interpretations of regulations by different individuals/entities, e.g. AMA interprets its own way, Payers interpret another. No consistency."

Clearinghouse: "The complaint process with CMS is effective, yet Payers continue to lag behind in dealing with compliance. Interpretation of the regulations is not absolute among Payers. From a Clearinghouse perspective, coding for individual Payer requirements out of compliance is a large roadblock for us. Also, Payers do not apply the same rules for paper claims and continue to require proprietary codes when submitting paper claims…"

Vendor: "The biggest roadblock we face is when a Payer doesn't follow HIPAA compliance. We have had to do many upgrades for various code sets because they do not follow the code set standard."

ROI and SUPPORT STRATEGIES

Providers and Payers were asked to comment on their strategies for Return on Investment (ROI) related to HIPAA initiatives. Almost one-third (30%) of Providers and 28% of Payers indicated that implementing ROI projects was part of their HIPAA compliance efforts. Of those pursuing ROI benefits, 83% of Providers and 91% of Payers planned to expand the organization's use of electronic HIPAA standard transactions. Transactions most frequently mentioned in relation to achieving ROI were the 835, 837, 270/271 and 276/277.

In light of the obstacles and challenges in achieving compliance and recognizing ROI, the good news is that many organizations are taking advantage of available resources to better understand the benefits of HIPAA. We are pleased to note that "HIPAAdvisory.com" was at the top of the ratings, followed by resources offered by CMS and National Associations (AHA, AHIMA, HIMSS, etc.). Although not included in our list of resources, many respondents commented that they have made extensive use of listserv-style discussion groups focusing on HIPAA.

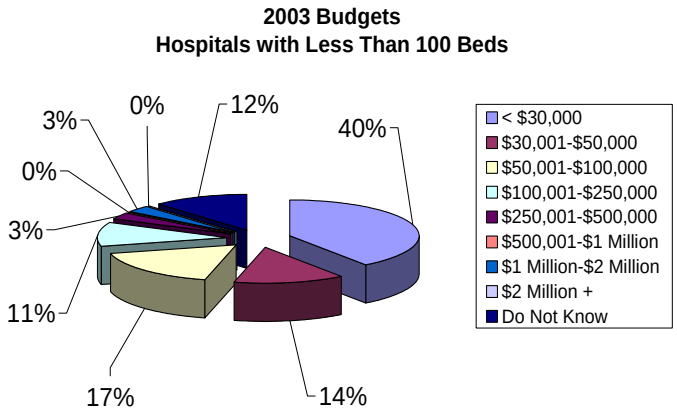
The Summer 2004 Survey results indicated that 42% of respondents across the industry (down from 49% in January 2004) are currently using outside consultants to support HIPAA compliance efforts, especially in the area of Security. Payers reported the greatest use of consultants – 56% of all Payers,

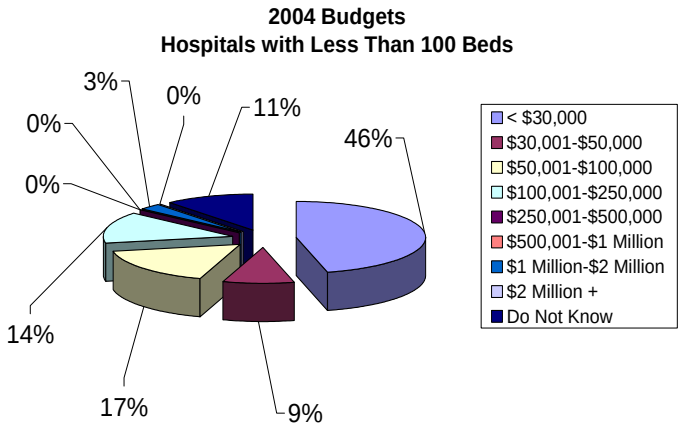
and 82% of large Payers. Of all respondents reporting the use of consultants, 58% had contracted for security assessments and implementation planning services.

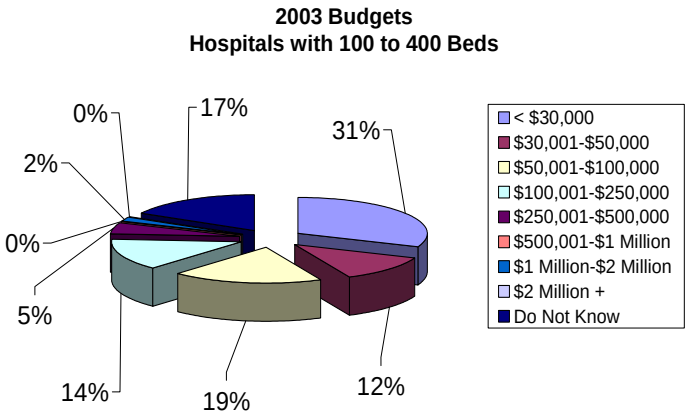
HIPAA BUDGET HIGHLIGHTS – 2003 and 2004

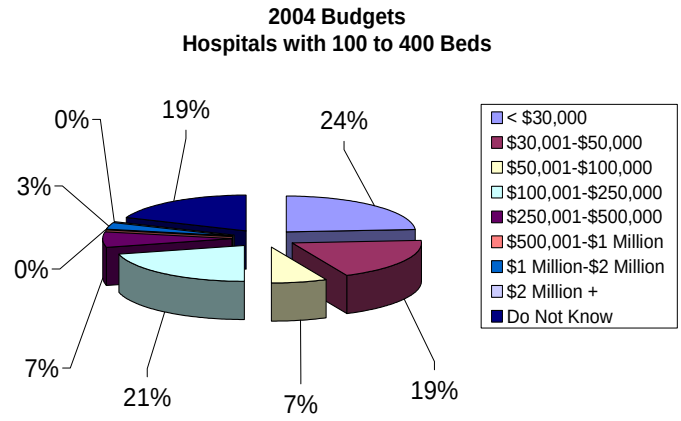
Graphical comparisons of hospital, Payer, and Vendor HIPAA budgets, by year, are offered below.

Hospital Budgets: 2003 vs. 2004

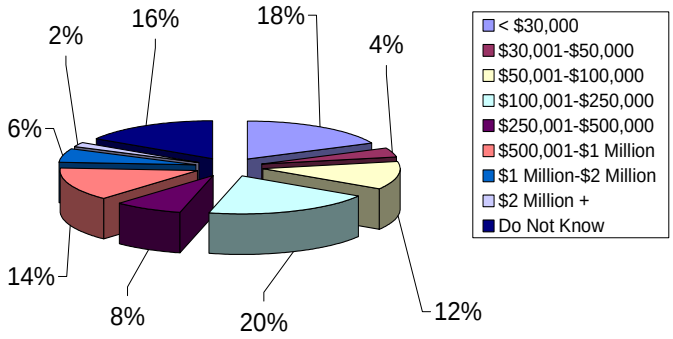




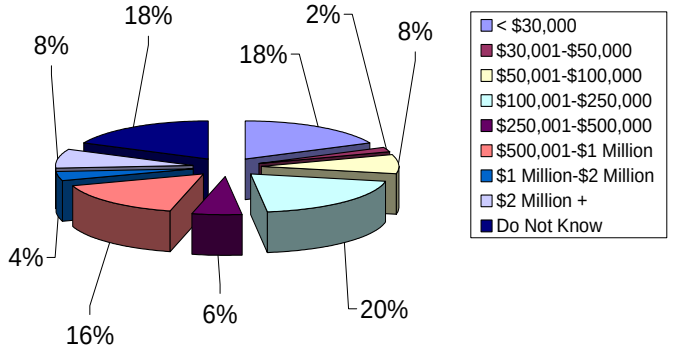




2003 Budgets
Hospitals with 400 or More Beds

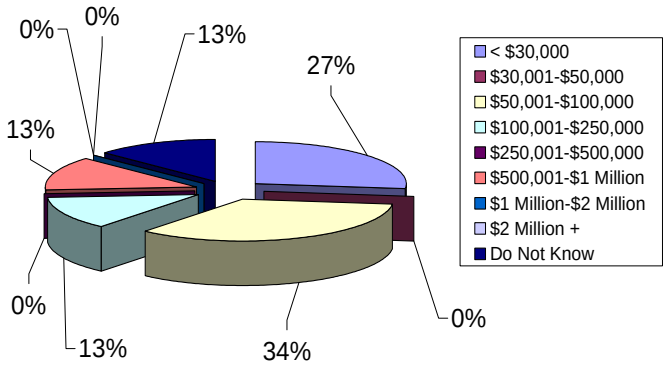


2004 Budgets
Hospitals with 400 or More Beds

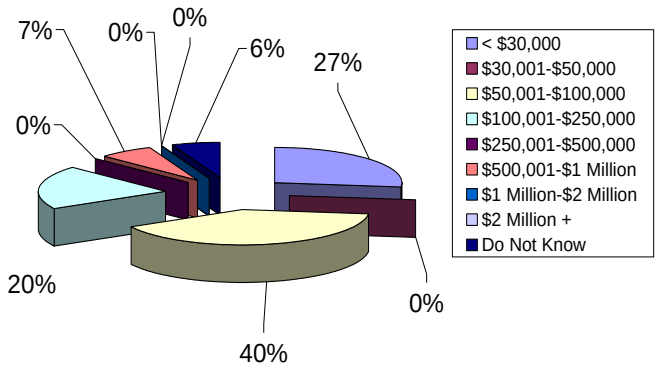


Payer Budgets: 2003 vs. 2004

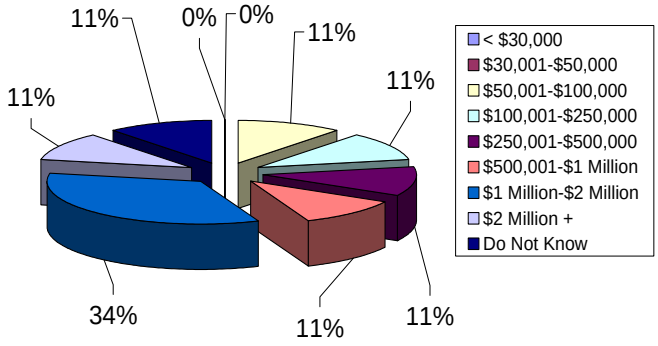
2003 Budgets
Payers Covering 150,000 or Fewer Lives



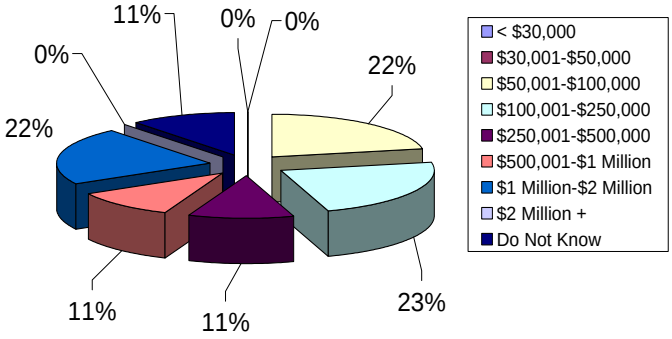
2004 Budgets
Payers Covering 150,000 or Fewer Lives



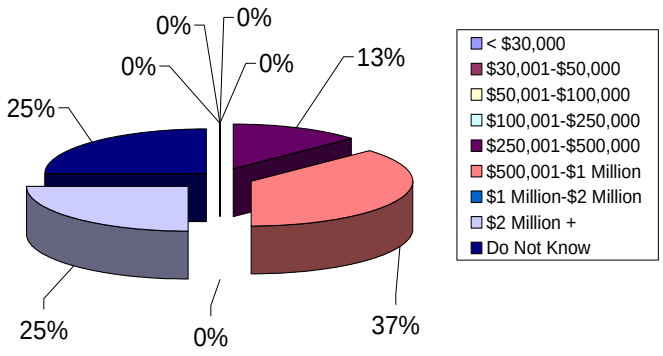
2003 Budgets
Payers Covering 150,000 to 500,000 Lives



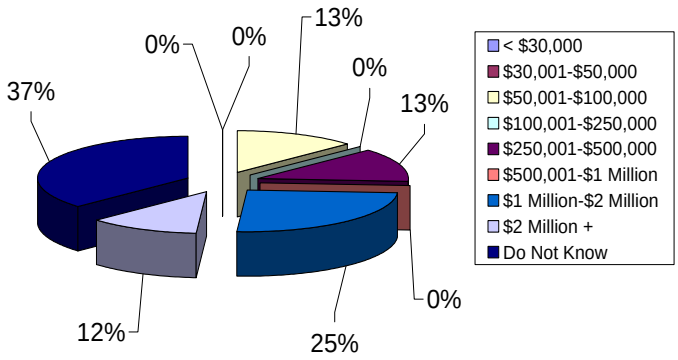
2004 Budgets
Payers Covering 150,000 to 500,000 Lives



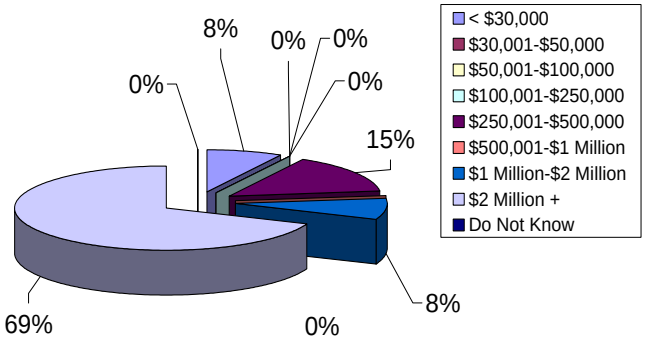
2003 Budgets
Payers Covering 500,000 to 1.5 Million Lives



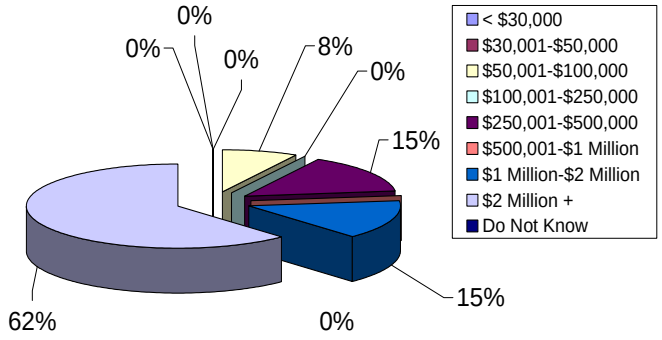
2004 Budgets
Payers Covering 500,000 to 1.5 Million Lives



2003 Budgets
Payers Covering More Than 1.5 Million Lives

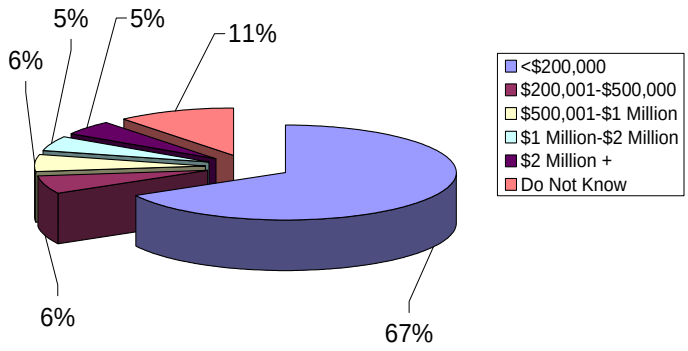


2004 Budgets
Payers Covering More Than 1.5 Million Lives

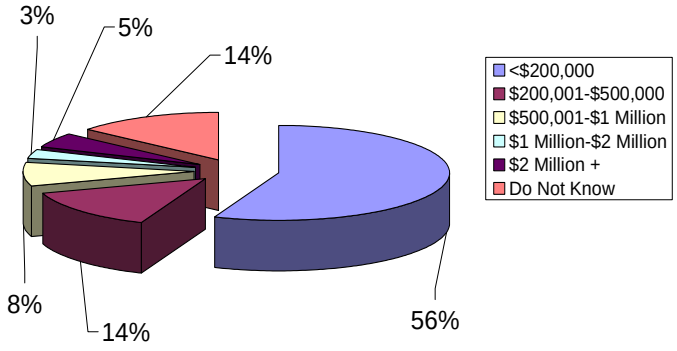


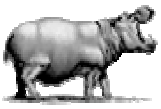
Vendor Budgets: 2003 vs. 2004

2003 Budgets
Vendors



2004 Budgets
Vendors





…HIPAA Knowledge…HIPAA Solutions

PHOENIX HEALTH SYSTEMS

Specialists in Healthcare Information Systems
Consulting and Outsourcing

- MIS Management and Outsourcing
- IT Strategic Planning and Procurement
- Systems Implementation
- HIPAA Privacy Implementation / Audit
- Information Security Implementation
- Revenue Enhancement / TCS ROI
- Clinical Transformation
- Patient Access Management
- Workforce / Executive Education

9200 Wightman Road, Suite 400
Montgomery Village, MD 20886
800 649-5225
http://www.phoenixhealth.com
http://www.hipaadvisory.com

HIMSS

Healthcare Information and
Management Systems Society

HIMSS (Healthcare Information and Management Systems Society) is the healthcare industry's membership organization exclusively focused on providing leadership for the optimal use of healthcare information technology and management systems for the betterment of human health.

Visit www.himss.org for more information.

230 East Ohio Street
Suite 500
Chicago, IL 60611-3269
312 664-HIMSS
312 664-6143
http://www.himss.org