# The State of HIPAA Privacy and Security Compliance

## April 2005

AHIMA
American Health Information Management Association®

A Report by the American Health Information Management Association

**Contents**



---

The American Health Information Management Association (AHIMA) is the premier association of health information management (HIM) professionals. AHIMA's 50,000 members are dedicated to the effective management of personal health information needed to deliver quality healthcare to the public. Founded in 1928 to improve the quality of medical records, AHIMA is committed to advancing the HIM profession in an increasingly electronic and global environment through leadership in advocacy, education, certification, and lifelong learning. For information about AHIMA, visit www.ahima.org.

Contributors:
Donald Asmonga, MBA
Jill Callahan Dennis, JD, RHIA
Meg Featheringham
Sue Fiorio
Kevin Gould
Scott MacKenzie
Cindy Nichols, RHIA, CHP
Dan Rode, MBA, FHFMA
Anne Zender, MA

American Health Information Management Association
233 N. Michigan Ave., Suite 2150
Chicago, IL 60601-5800
www.ahima.org

# Executive Summary

In 2004, the American Health Information Management Association (AHIMA) undertook its first survey to gain an understanding of where healthcare organizations stood with regard to implementing the privacy and security rules of the Health Insurance Portability and Accountability Act (HIPAA). The survey results were released in April 2004, one year after the implementation of the final privacy rule.

AHIMA has again surveyed healthcare privacy officers and others whose jobs relate to the HIPAA privacy function. This time the survey looked not only at compliance with the privacy rule but also with the security rule, which goes into effect on April 21, 2005. AHIMA hopes the results of the survey will reinforce the importance of protecting the privacy, confidentiality, and security of personal health information. It also hopes to help the industry understand the areas of privacy and security implementation that are most difficult and may need more study.

AHIMA releases the results of this research in conjunction with the second annual National Health Information Privacy and Security Week, April 10-16, 2005. AHIMA is sponsoring National Health Information Privacy and Security Week to raise awareness among healthcare professionals, their employers, the media, and the public regarding the importance of protecting the privacy, confidentiality, and security of personal health information (PHI).

## Profile of Respondents

Although the respondents as a whole work in a variety of settings, in many places this report focuses on those with the largest numbers: the 51 percent of respondents who are employees of hospitals and health systems (H&HS).

Fifty-one percent of the 1,140 survey respondents consisted designated privacy or security officials and 26 percent who serve on HIPAA privacy or security teams or committees. Others functioned as the privacy or security officer without the official title.

## Meeting Compliance

Most institutions report they are fully compliant with the privacy regulations. A comparison between the 2004 and 2005 surveys shows full privacy compliance at 40 percent for hospitals and health systems compared to last year's 23 percent. Overall, 91 percent of all respondents considered themselves more than 85 percent compliant with the privacy regulation.

## Compliance Challenges

Organizations are complying with the regulations, but not without some difficulty in addressing various requirements.

The survey asked responders to identify their "number one" ongoing problem associated with their facility's HIPAA privacy procedure. Education and training was consistently mentioned as the main concern of the responders across all segments of the hospital and health system population.

Organizations of all size raised the privacy requirement for accounting for disclosures as the most difficult to deal with and one that has very little value given the number of actual requests for such accountings. This provision topped the list when H&HS respondents were asked to identify which aspects of the privacy rule need to be modified by the federal government:

- Accounting for disclosures (61 percent)
- Access and release of information to relatives or "significant others" (22 percent)
- Business associate requirements (20 percent)
- Release of information to law enforcement (17 percent)

When asked whether they were having difficulties implementing and enforcing specific provisions of the privacy rule, most respondents reported only slight or no difficulties with most of the requirements. However, a few requirements produced significant concerns:

- Accounting for disclosures
- Access and release of information to law enforcement
- Access and release of information to relatives or patients' "significant others"
- Release of information for research protocols
- Access and release of information for subpoenas versus court orders
- Business associate agreements

## State Pre-emption

The 2005 survey data shows a small increase in the number of respondents who find that the impact of the HIPAA allowance for state pre-emption has caused difficulties, as indicated by 25 percent of the respondents, compared to 21 percent in 2004. Respondents from larger organizations may be more likely to experience problems.

H&HS respondents most frequently encountered problems such as state requirements related to consents, access and release of information to law enforcement, access and release for subpoenas or court orders, access and release of information to relatives or "significant others," and business associate requirements.

## Reactions to HIPAA Privacy

The survey asked several questions designed to gauge patient reaction to HIPAA privacy policies and whether facilities have changed their notice of privacy practices in response to patient reactions. It also looked at patient complaints and staff reactions to the policies.

Fifty percent of H&HS respondents felt patients were somewhat or very supportive of HIPAA privacy policies, compared to 54 percent in 2004.

But many facilities have encountered patient complaints, even if they are the result of misunderstandings. The results reveal the nature of many common complaints, which range from public conversations to inappropriate disclosure of PHI to family members or patient representatives. Privacy officers report that it is not always easy to determine just who the patient's representative is.

## Handling Consents and Requests

Under HIPAA, individuals have the right to ask for an accounting of all disclosures of personal health information for purposes other than treatment, payment, or healthcare operations. When asked to indicate how many requests for an accounting they have received, most commonly H&HS respondents had received "only a few" or no requests for an accounting (67 percent reported receiving no requests). Larger facilities were more likely to report more than 15 requests in the past 12 months.

## Security: The Next Challenge

Do facilities believe they are compliant with HIPAA security? Many entities say they are on the road to full compliance by the April 21, 2005, implementation date. At the time of the survey (January 2005), the implementation deadline was still several months away. Seventeen percent of all responders described themselves as completely compliant, 43 percent described themselves as 85 to 95 percent compliant, 26 percent felt they were about 50 percent compliant, and 12 percent felt they were less than 50 percent compliant. Where facilities were behind on implementation, there was generally a resource conflict with other necessary information technology (IT) projects.

Respondents were asked to identify the number one problem identified and corrected during the security implementation process. Not surprisingly, many identified the top issue as access and the tracking of access. Other issues were the more technical aspects of security related to IT systems. As with the implementation of the HIPAA privacy regulations, work done on security has also helped 54 percent of all responding organizations uncover problems with business practices or procedures.

As in 2004, the survey asked if the facility had designated a security officer. Eighty-eight percent of H&HS respondents responded positively, a slight increase over the 80 percent response in 2004. Of those with a full-time security officer, facilities reported that an IS/IT employee was most likely to fill the role. Health information management (HIM) professionals were the second most likely to occupy the security officer position.

## Privacy and Security Training

Training and education have been important concerns for privacy officers, so for benchmarking purposes the survey asked some questions related to training and HIPAA. Sixty-two percent of all respondents reported new employee privacy training being done in-house by the privacy or education officer. In-house instruction and Web-based instruction topped the list in most facilities, except where the smallest facilities favored video instruction over the Web.

HIPAA also requires security training for all personnel and volunteers. Forty-five percent of all respondents indicated that their facility had developed its own educational program for initial training. As with privacy training, online education was also popular.

## Outsourcing

The survey asked some questions related to outsourcing to highlight the need to protect personal health information. While not a definitive snapshot of all healthcare outsourcing, the results point to issues that could arise in any future networking of personal health information. The survey asked whether facilities outsource any HIM functions. While 42 percent of all respondents answered “yes,” the results vary across facility size. Transcription and release of information were the two most frequently outsourced HIM functions. Data does not indicate whether these functions were outsourced to companies out of state, out of the country, or just out of the facility.

## Conclusion

Two years after the implementation of the HIPAA privacy rule, the AHIMA survey finds the following conclusions:

- **The majority of facilities are significantly compliant with privacy and expected to be compliant with HIPAA security** as well. The responses, however, indicate that privacy officers want the industry to know that resources are needed to maintain compliance.
- While facilities may expect to be "done" with HIPAA, privacy officers understand the **need for renewed commitment to education and training for ongoing success**. Again, the respondents believe that privacy compliance is the duty of everyone in an organization, not just those charged with overseeing the process.
- Most respondents have had little or no difficulty implementing provisions of the privacy rule, but reports of difficulties with a handful of requirements suggest **areas where more education or refinement may be necessary**. Certain areas continue to present operational challenges, such as:
    - -Accounting for disclosures
    - -Access and release of information to law enforcement
    - -Access and release of information to relatives or patients' "significant others"
    - -Release of information for research protocols
    - -Access and release of information for subpoenas versus court orders
    - -Business associate agreements.
- **Protecting personal health information continues to be an important goal**, as emerging issues such as outsourcing suggest.

# Survey Results and Analysis

## About the 2005 Survey

In 2004, the American Health Information Management Association (AHIMA) surveyed healthcare professionals to gain an understanding of where their organizations stood with regard to implementing the privacy and security rules of the Health Insurance Portability and Accountability Act (HIPAA). The survey results were released in April 2004, a year after the implementation of the final privacy rule.

AHIMA has again surveyed healthcare privacy officers and others whose jobs relate to the HIPAA privacy function. This time the survey looked not only at compliance with the privacy rule but also with the security rule, which goes into effect April 21, 2005. AHIMA hopes the results of the survey will both reinforce the importance of protecting the privacy, confidentiality, and security of personal health information and help the industry understand the areas of implementation that are most difficult and may need more study.

AHIMA releases the results of this research in conjunction with the second annual National Health Information Privacy and Security Week, April 10-16, 2005.

AHIMA conducted the survey in January 2005, with the assistance of an impartial third-party market research firm. E-mail invitations were sent to AHIMA members who were considered most likely to have participated significantly in the HIPAA implementation process and others who had participated in various HIPAA-related educational opportunities provided by AHIMA.

The survey received 1,140 qualified responses. Similar to the 2004 survey, **51 percent of responses came from those working in a hospital setting. In many cases, this report's analysis and breakdowns by size focus on this group of respondents**.

The remainder of responses came from integrated delivery systems, ambulatory care, physician offices, behavioral, mental and home health, long-term care, and other settings. The responses are also diverse geographically; qualified responses were received from all 50 states.

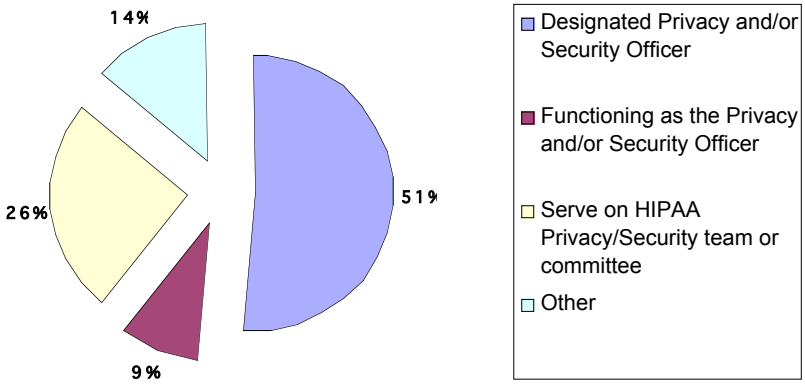
AHIMA has a long history of protecting health records and information that dates back to the founding of the association in the 1920s. For more than 75 years, AHIMA has taken on this charge in a number of different healthcare settings. In many cases, AHIMA members have been charged with the HIPAA privacy and security mandates.

With this survey, as with the 2004 survey, AHIMA seeks to educate the public and the industry on issues that have been and will need to be addressed. The goal is to maintain and increase public trust in a healthcare system that needs to maintain and protect personal health information to provide maximum benefits to its patients.

## Respondents

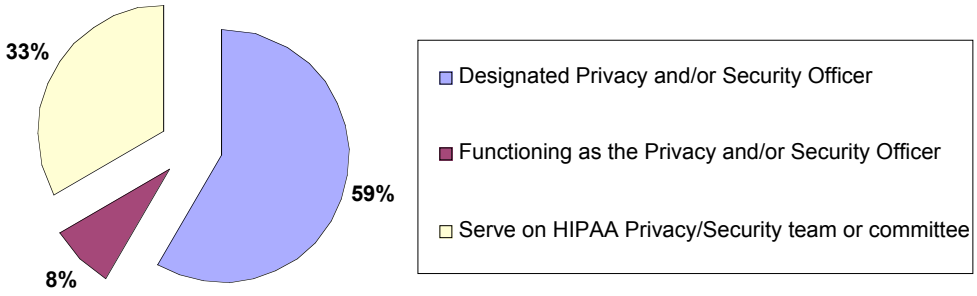
Of the total 1,140 respondents, 51 percent were designated as either the privacy or security officer for their organization. Another 9 percent indicated that they were functioning as the privacy or security officer but without the formal title–most likely because they held the position part time or in combination with other duties. Another 26 percent indicated that they served on a privacy or security team or committee, while 14 percent answered "other." AHIMA is aware that a number of HIM department directors or assistants often take on the privacy officer role because they have expertise in this area. It appears, therefore, that 60 percent of all respondents were directly involved in the privacy or security functions of their organization.

**All Respondents**




Similarly, among respondents from hospitals and health systems (H&HS), almost two-thirds of respondents were privacy or security officers, while the remaining third served on a HIPAA task force or committee. These results are consistent with those of the 2004 survey.

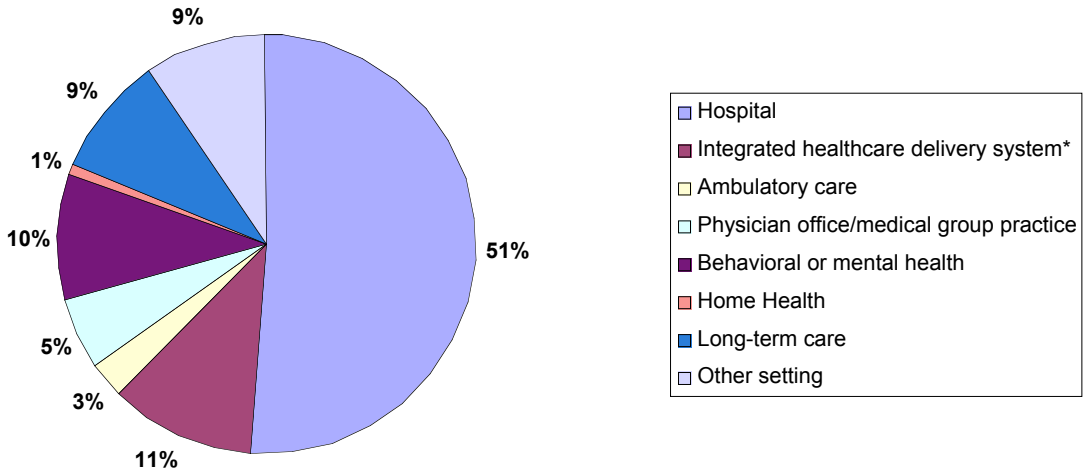
**Hospital and Health Systems Respondents**



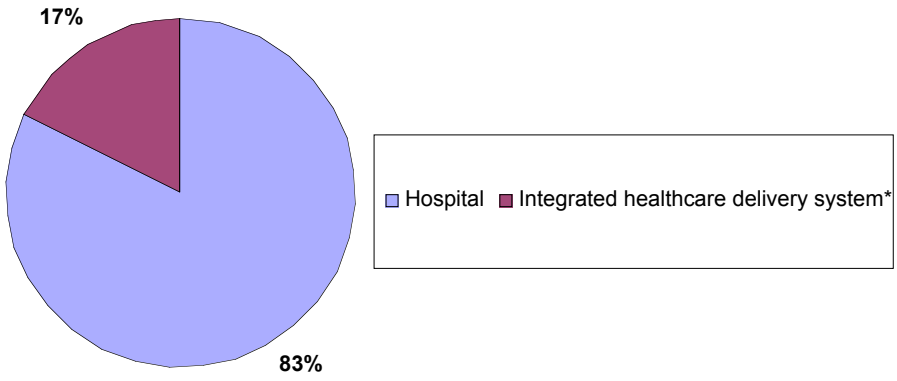

## Types of Facilities

Hospitals and health systems made up 51 percent of respondents, with the remainder in other settings (the largest representation being long-term care [9 percent] and behavioral or mental health [9 percent]). Other areas represented include ambulatory care, physician offices, and home care. The H&HS breakdown shows 83 percent of the respondents indicating they work in hospitals and 17 percent in integrated healthcare delivery systems.

**Facility Types**




**Hospitals and Health Systems**




For the purposes of this survey, respondents are categorized by numbers of admissions/discharges during the last calendar year (as reported by the respondents). The categories are:

- More than 50,000 admissions/discharges (A/D) (7 percent of respondents)
- 20,000-49,999 admissions/discharges (13 percent)
- 10,000-19,999 admissions/discharges (11 percent)
- 5,000-9,999 admissions/discharges (12 percent)
- 2,000-4,999 admissions/discharges (15 percent)
- Fewer than 2,000 admissions/discharges (39 percent)

## Privacy: Who's in Charge?

When asked **whether their facility has a privacy officer**, 40 percent of all respondents had a full-time officer, while 53 percent had a part-time officer. A breakdown by admissions and discharges shows that the larger a facility is, the more likely it is to have a full-time privacy officer.

| Privacy Officer? | >50,000 A/D | 20,000-49,999 A/D | 10,000-19,999 A/D | 5,000-9,999 A/D | 2,000-4,999 A/D | <2,000 A/D |
|---|---|---|---|---|---|---|
| Full-time | 61.4 % | 51.1% | 40.5% | 38.1% | 27.8% | 24.7% |
| Part-time | 36.4% | 47.8% | 57.1% | 60.8% | 69.1% | 70.8% |
| No | 2.3% | 1.1%% | 2.4% | 1% | 3.1% | 4.5% |

Even then, however, the largest reporting group indicates only 61 percent have a full-time officer, while in the smallest group just under 25 percent (24 percent) have a full-time privacy officer. A large majority of total respondents (91 percent) indicate that the part-time or full-time status of their privacy officer has not changed in the last year.

A small number of facilities (5 percent) still report having no privacy officer at all. This is cause for concern, as the privacy rule requires that a covered entity designate a privacy official.

**How busy a part-time privacy officer might be** apparently depends on facility size. Facilities with fewer than 5,000 admissions/discharges a year indicated that about 85 percent of their part-time privacy officers spend less than 25 percent of their total time dealing with privacy issues, while very large facilities indicate that more than 27 percent of their part-time officers spend more than 50 percent of their time engaged in privacy matters.

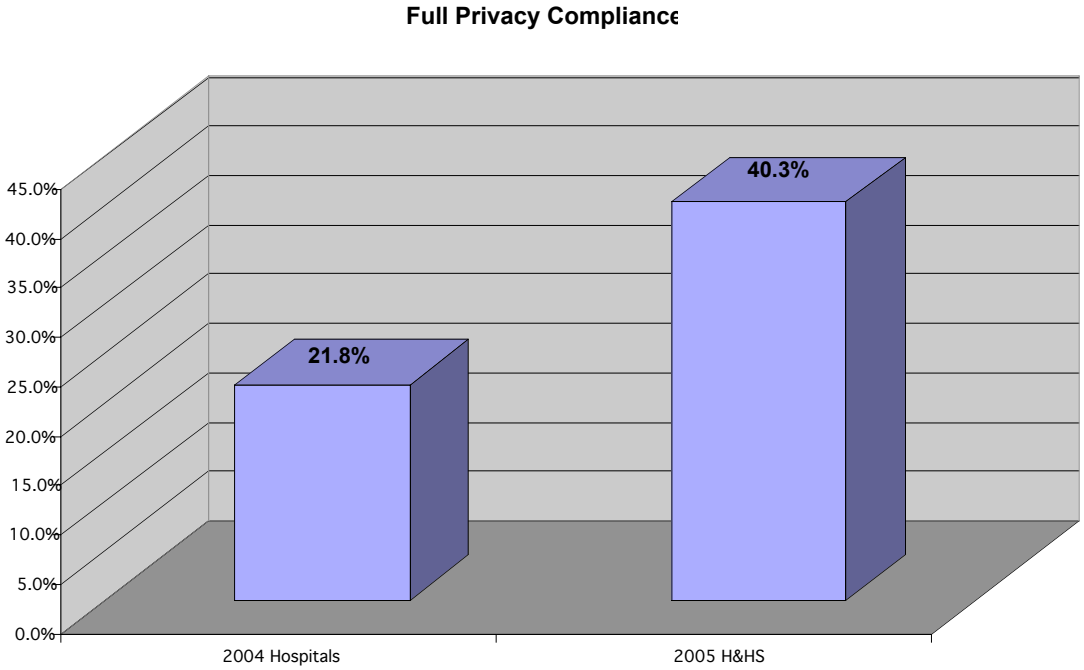
Another question asked whether the respondents' facility had a **committee or task force related to privacy**. Eighty-one percent of H&HS responded that they did, an 8 percent drop since 2004. Ninety-five percent of facilities with the highest number of admissions/discharges reported having such a committee.

In written comments, many respondents noted a lack of time to complete what they now view as additional duties associated with the privacy rule. Respondents reported difficulty staying abreast of new frequently asked questions associated with the privacy rule, state changes, employee changes (requiring training), reminding employees of the privacy requirements, addressing the security rule, and so forth. Similarly, many of these individuals felt that their lack of time and to some extent resources was due to a lessened lack of commitment to the privacy compliance process by their institution. Others, however, noted that the problem was less a lack of a commitment than competition for resources and time for a variety of other projects.

## Privacy: How Compliant Are We?

Respondents were asked: "**In your opinion, how compliant is your facility with the HIPAA privacy requirements?**"

A comparison between the 2004 and 2005 surveys shows full compliance at 40 percent for H&HS over last year's 22 percent level. (Overall, 91 percent of all respondents reported being 85 percent or more compliant.) This high level of compliance means that these facilities may be better prepared in future to move toward the bigger challenge of addressing privacy in regional networks envisioned by the Department of Health and Human Services and groups like Connecting for Health and the eHealth Initiative.




Unfortunately, a year after the compliance deadline for hospitals and health plans, a small number indicate that they are 50 percent compliant or less. In 2004 respondents indicated 7 percent of H&HS respondents were less than 50 percent compliant, while the percentage in 2005 is 4 percent. A small percentage of less compliant responses exists in almost all size categories.

| Compliance | >50,000 A/D | 20,000-49,999 A/D | 10,000-19,999 A/D | 5,000-9,999 A/D | 2,000-4,999 A/D | <2,000 A/D |
|---|---|---|---|---|---|---|
| Less than 50?% | 0% | 1.1% | 1.2% | 0% | 0% | 2% |
| About 50% | 0% | 2.2% | 3.6% | 4.1% | 3.1% | 4.6% |
| > 85% | 100% | 96.7% | 95.1% | 95.9% | 96.9% | 93.4% |

Many others report 100 percent compliance, but as other data in the study indicate, not without some difficulty in addressing various HIPAA compliance requirements.

## Difficulties with HIPAA Privacy Requirements

The survey asked whether respondents were having difficulties implementing and enforcing specific provisions of the privacy rule. Most H&HS respondents reported no or only slight difficulties with most of the requirements. However, a few requirements produced significant concerns.

Under HIPAA, individuals have the right to ask for an accounting of all disclosures of personal health information for purposes other than treatment, payment, or healthcare operations. **The accounting for disclosures requirement** has received a lot of attention. The question of difficulty may depend on how often an organization is asked to provide such an accounting.

| Difficulty | >50,000 A/D | 20,000-49,999 A/D | 10,000-19,999 A/D | 5,000-9,999 A/D | 2,000-4,999 A/D | <2,000 A/D |
|---|---|---|---|---|---|---|
| None | 35.6% | 29.3% | 42.9% | 30.6% | 44.3% | 42.6% |
| Slight | 26.7% | 33.7% | 28% | 37.2% | 31.5% | 37.1% |
| Moderate | 27.7% | 28.8% | 20.2% | 23% | 20.2% | 16.5% |
| Extreme | 10% | 8.2% | 8.9% | 9.2% | 4% | 3.8% |

Larger facilities and especially health systems report difficulty dealing with **access and release of information to law enforcement**, due to multiple jurisdictions and other issues.

| Difficulty | >50,000 A/D | 20,000-49,999 A/D | 10,000-19,999 A/D | 5,000-9,999 A/D | 2,000-4,999 A/D | <2,000 A/D |
|---|---|---|---|---|---|---|
| Moderate | 13.35% | 3.85% | 4.8% | 5.1% | 7.3% | 5.2% |
| Extreme | 6.65% | 4.85% | 0% | 3% | 3% | 1.3% |

Comments made by responders indicate that most law enforcement personnel were not made aware of the HIPAA regulation in advance of the compliance date and were unhappy to learn of the requirements when they requested information. Clearly more of an effort should have been made to educate the law enforcement community.

Some respondents reported difficulty with **access and release of information to patients' relatives or patients' "significant others."**

| Difficulty | >50,000 A/D | 20,000-49,999 A/D | 10,000-19,999 A/D | 5,000-9,999 A/D | 2,000-4,999 A/D | <2,000 A/D |
|---|---|---|---|---|---|---|
| Moderate | 14.4% | 4.4% | 9% | 10.8% | 11.8% | 6.8% |
| Extreme | 1.1% | 3.3% | 3% | 4.7% | 2.6% | 0.3% |

Anecdotal comments mentioned problems related to release of information to patients' relatives, particularly verbally as opposed to release of the paper or electronic record. Comments indicated that staff could not easily determine who in the "family" should or should not get information and in what setting. Some suggested that the requirement is too ambiguous and does not take into consideration all the situations that clinical staff especially might find themselves in as they provide services in close proximity to relatives or significant others. The data show this is a problem for all sizes of facilities.

Considerable discussion has occurred in the last year related to **information being released for research protocols**. The results show that the largest group has listed this as an issue.

| Difficulty | >50,000 A/D | 20,000-49,999 A/D | 10,000-19,999 A/D | 5,000-9,999 A/D | 2,000-4,999 A/D | <2,000 A/D |
|---|---|---|---|---|---|---|
| Moderate | 11.1% | 3.9% | 3.1% | 2.6% | 1% | 3.7% |
| Extreme | 2.2% | 0.5% | .06% | 1.6% | 0% | 0.4% |

Larger facilities are more likely to be involved in a research program or protocol. For more than 10 percent to indicate that they have a problem in this area would suggest that concerns have been raised in a variety of research circles and that this issue continues to require attention.

Some respondents also reported difficulty with **access and release of information for subpoenas versus court orders**.

| Difficulty | >50,000 A/D | 20,000-49,999 A/D | 10,000-19,999 A/D | 5,000-9,999 A/D | 2,000-4,999 A/D | <2,000 A/D |
|---|---|---|---|---|---|---|
| Moderate | 4.4% | 3.8% | 3.6% | 6.1% | 6.7% | 3.25% |
| Extreme | 4.4% | 1.7% | 0% | 2% | 1.5% | 1.25% |

Certainly the problems here are not as critical as with law enforcement. We know from a variety of discussions that many problems with subpoenas and court orders occurred because attorneys and courts were unfamiliar with the HIPAA regulations. This might be the case for facilities with fewer than 10,000 admissions/discharges, especially in locations where HIPAA education for non-HIPAA entities was not available.

**Business associate agreements** also cause concern for a variety of reasons.

| Difficulty | >50,000 A/D | 20,000-49,999 A/D | 10,000-19,999 A/D | 5,000-9,999 A/D | 2,000-4,999 A/D | <2,000 A/D |
|---|---|---|---|---|---|---|
| Moderate | 7.8% | 4.4% | 4.2% | 5.2% | 11.9% | 5.8% |
| Extreme | 3.3% | 1.1% | 1.8% | 2.1% | 2.6% | 1.3% |

The groups indicating moderate or more serious problems vary. Because health systems make up a considerable amount of the greater than 50,000 A/D group, the problem may have as much to do with volume as complexity. Why those in the 2,000 to 4,999 A/D group seem to have more difficulty than other small groups is not clear.

The survey asked, "**Which areas of the HIPAA privacy rule do you believe need to be modified by the federal government**?" Unsurprisingly, H&HS responses to this question vary according to the size of the facility. The following were identified by 15 percent or more of respondents as problems needing modification:

- Accounting for disclosures (61 percent)
- Access and release of information to relatives or "significant others" (22 percent)
- Business associate requirements (20 percent)
- Release of information to law enforcement (17 percent)

| Area that Should Be Modified | >50,000 A/D | 20,000-49,999 A/D | 10,000-19,999 A/D | 5,000-9,999 A/D | 2,000-4,999 A/D | <2,000 A/D |
|---|---|---|---|---|---|---|
| Release to law enforcement | 28% | 17.6% | 15.9% | 19.4% | 15.6% | 13.1% |
| Acc/rel of PHI to relatives | 17.8% | 13.2% | 23.2% | 20.4% | 35.4% | 25.5% |
| Accounting for release of PHI | 75.6% | 75.8% | 63.4% | 63.3% | 51% | 52.3% |
| Business associate agreements | 33.3% | 13.2% | 11% | 18.4% | 20.8% | 29.4% |

As in 2004, accounting for disclosures remains a top issue for all organizations. The data show that the number of requests for an accounting is very small (see page 17). But the administrative work facilities must do to be able to respond to requests should also be taken into consideration.

## Other Privacy Concerns

The survey asked responders to identify their number one ongoing problem associated with their facility's HIPAA privacy procedures. Education and training was consistently mentioned as the main concern of the responders across all segments of the H&HS population. The consensus appears to be that ongoing education and retraining is an issue and that there is less support and fewer resources for such activities. Privacy officers and others related to the privacy effort say that there is less support for training efforts now that HIPAA privacy is in place.

Responders also noted a rise in the inappropriate verbal discussion of a patient's personal health information and some sloppiness regarding keeping records out of sight on nursing stations and in

similar situations. This evidence of slipping back into old habits could be the result of minimal efforts and resources being directed toward ongoing training and reminders.

Keeping personal health information private in small institutions and in small communities was mentioned several times. Privacy officers raise concerns that clinicians are not always in a position to determine just who in a family should or should not be communicated with. The patient or individual is also not always able to identify his or her wishes in this regard, and the families themselves may be in conflict regarding this issue.

Access to personal health records by employees was also raised as an issue. Some of these concerns may be addressed by the implementation of the security rule. But for the combination of security and privacy rules to work, it needs the visible support of a facility's leadership, through training, appropriate resources, clear policies on access and disclosure, and discipline when necessary.

## The Impact of State Pre-emption

The 2005 data show a small increase in the number of H&HS respondents who say that the impact of the HIPAA allowance for **state pre-emption** has caused difficulties, as indicated by 25 percent of the respondents, compared to 21 percent in 2004. The categories representing larger groups may be more likely to experience problems as they include systems that are in more than one state. Some pre-emption issues relate more to where a facility is located and where its patients live than to size. In either case, developers of regional or national health networks that cross state borders should be aware of this statistic.

| **Pre-emption** | **>50,000 A/D** | **20,000-49,999 A/D** | **10,000-19,999 A/D** | **5,000-9,999 A/D** | **2,000-4,999 A/D** | **<2,000 A/D** |
|---|---|---|---|---|---|---|
| Yes | 28.9% | 37.4% | 14.5% | 28.6% | 17.9% | 23.4% |
| No | 71.1% | 62.6% | 85.5% | 71.4% | 82.1% | 76.6% |

As a follow up to this question, the survey asked respondents to identify the areas causing them the most problems. The top five answers from H&HS respondents were:

| **Problem Area** | **2004** | **2005** |
|---|---|---|
| State requirements related to consents | 57.1% | 57.2% |
| Access/release of PHI to law enforcement | 30.7% | 40.8% |
| Access/release for subpoenas/court orders | 27.9% | 34.9% |
| Access/release of PHI to relatives/"significant others" | 33.6% | 38.2% |
| Business associate requirements | 20% | 24.3% |

The state requirement for consents to use or disclose personal health information for treatment, payment, and healthcare operations (TPO) remains high; however, many hospitals and systems require such consents on their own. Anecdotal evidence seems to indicate that problems may occur when there is a difference of opinion on the need for consents between providers (for example, when one provider requests information for TPO and the sending provider will not release the information until a consent can be given).

State consent requirements appear to be an issue for smaller facilities (10,000 or fewer admissions/discharges) than for larger ones, although even the largest groups indicated a problem for more than 30 percent of the respondents. Law enforcement issues, however, appear to be a bigger problem for the largest groups and subpoenas/court orders for those in the middle of the breakdown. This is an area that has been addressed with limited success by the National Committee on Vital and Health Statistics and appears to need more attention.

The issue of releasing information to relatives and "significant others" appears here again. This problem will have to be watched, for there is no clear indication of how to resolve the problem of determining the interrelationships of patients with family and friends.

| Area of Difficulty | >50,000 A/D | 20,000-49,999 A/D | 10,000-19,999 A/D | 5,000-9,999 A/D | 2,000-4,999 A/D | <2,000 A/D |
|---|---|---|---|---|---|---|
| State consents for TPO | 30.8% | 47.1% | 25% | 72.4% | 66.7% | 71.4% |
| Law enforcement | 69.2% | 41.2% | 33.3% | 31% | 27.8% | 51.4% |
| Subpoenas/court orders | 23.1% | 29.4% | 41.7% | 48.3% | 33.3% | 37.1% |
| PHI to relatives or sig. others | 30.8% | 26.5% | 50% | 34.5% | 61.1% | 42.9% |
| Business associate agreements | 23.1% | 26.5% | 16.7% | 17.2% | 22.2% | 37.1% |
| Post-care release of information to patient or relatives | 30.8% | 29.4% | 16.7% | 31% | 44.4% | 25.7% |

## Reactions to HIPAA Privacy

The survey asked several questions designed to gauge patient reaction to HIPAA privacy policies and whether facilities have changed their notice of privacy practices in response to patient reactions. The survey also looked at patient complaints and staff reactions to the policies.

**Patient reactions to the privacy requirements** have been a subject of ongoing discussion among some healthcare policy makers. The data only reflect how H&HS staff members perceive patient reaction. However, the changes between the 2004 and 2005 survey results will add to the discussion. They could be the result of patients having nine months of experience with various providers' privacy requirements.

| Reaction to Privacy Policies | 2004 | 2005 |
|---|---|---|
| Very supportive of efforts to protect the privacy of their information | 22.9% | 17.7% |
| Somewhat supportive | 31.6% | 33% |
| Indifferent | 35.5% | 40.7% |
| Not very supportive | 6.2% | 7.6% |
| Not at all supportive | 0.8% | 1% |
| Uninformed/Confused | 3% | N/A |

The next question asked whether **patients understand their rights and the facility's responsibilities**. It is clear that more consumer education in this area might be appropriate as almost a third of H&HS patients seem to have little understanding of privacy rights and facility responsibilities.

| | |
|---|---|
| Complete understanding | 3% |
| Some understanding | 63.6% |
| Very little understanding | 28.7% |
| No understanding | 1.6% |
| Not sure | 3.1% |

Nineteen percent of all respondents indicate that their facilities have **changed their privacy notices** since HIPAA privacy implementation. Most of the changes were made to clarify language and make the notice more understandable. Often changes were caused by demographic changes, telephone numbers, title changes, and so forth. This relatively high percentage is a sign that organizations are listening to the needs of their patients and making a good faith effort to maintain an accurate notice of privacy practices.

HIPAA requires facilities to have a process for handling complaints regarding its privacy practices. But some complaints are the result of misunderstandings rather than a violation of the rule. The survey asked if facilities had received any **complaints** regarding the HIPAA rule or their rights. A number of facilities reported complaints. A H&HS breakdown shows:

| **Complaints** | **>50,000 A/D** | **20,000-49,999 A/D** | **10,000-19,999 A/D** | **5,000-9,999 A/D** | **2,000-4,999 A/D** | **<2,000 A/D** |
|---|---|---|---|---|---|---|
| Yes | 80% | 78% | 75% | 78.6% | 66% | 42.9% |
| No | 20% | 22% | 25% | 21.4% | 34% | 57.1% |

The survey asked whether the respondents believed the difference between federal HIPAA requirements and state laws caused any complaints. H&HS responses varied.

| **Complaints: federal vs. state** | **>50,000 A/D** | **20,000-49,999 A/D** | **10,000-19,999 A/D** | **5,000-9,999 A/D** | **2,000-4,999 A/D** | **<2,000 A/D** |
|---|---|---|---|---|---|---|
| Yes | 13.9% | 15.5% | 14.3% | 10.3% | 14.3% | 6% |
| No | 86.1% | 84.5% | 85.7% | 89.7% | 85.7% | 94% |

Next the survey asked for the types of complaints facilities received. The H&HS responses can best be described in terms of facility size.

**50,000+ admissions and discharges:** Most of the complaints in this category related to patient concern that some facility staff, family member, or other inappropriate party had been given or had access to personal health information that the patient believed was inappropriate. Also mentioned were conversations between staff members regarding the individual or another patient's personal health information that was overheard by the person making the complaint. Some employees complained that their records had been accessed by other employees. Finally, there were issues related to the amendment process; most appeared to be due to patient misunderstanding of the process itself.

**20,000-49,999 admissions and discharges:** This segment echoed many of the complaints noted above, but raised more issues related to discussions the patient believed occurred with inappropriate family members. Other complaints surfaced regarding release of information.

**10,000 – 19,999 admissions and discharges:** This category also echoed those above, but facilities in this group more often mentioned concerns raised by not understanding the rule itself. But clearly patients did understand the rules enough to be concerned about staff conversations with each other and with the patient that were not necessarily occurring in private quarters. Facilities in this category also mentioned complaints regarding what the patient believed to be an inappropriate release of information.

**Under 9,999 admissions and discharges:** This category also reflected concerns mentioned above. However, complaints regarding overheard conversations appear to increase in smaller facilities, as does the concern that facility employees in small communities are discussing an individual's encounter with members of their family and neighbors. The impression is that other than employee retraining and education, there is little a privacy officer can do to address these concerns. The small facilities also more often reported confusion among patients concerning the rights and responsibilities provided by the HIPAA rules. Because the rules appear to be met in different ways by different HIPAA entities, leaving the individual confused, facilities would do well to attempt to reach consensus among themselves.

Eighteen percent of H&HS respondents felt that **staff** at their facility were indifferent or not very supportive of HIPAA privacy efforts. The indifference appears to be higher in smaller facilities and could also relate to the need for education and re-education.

| Staff Reaction | >50,000 A/D | 20,000-49,999 A/D | 10,000-19,999 A/D | 5,000-9,999 A/D | 2,000-4,999 A/D | <2,000 A/D |
|---|---|---|---|---|---|---|
| Very supportive | 35.6% | 40.7% | 37.3% | 26.5% | 32.3% | 32.2% |
| Somewhat supportive | 57.8% | 44% | 47% | 52% | 41.7% | 46.7% |
| Indifferent | 4.4% | 4.4% | 12% | 15.3% | 16.7% | 12.5% |
| Not very supportive | 2.2% | 11% | 3.6% | 6.1% | 9.4% | 8.6% |
| Not at all supportive | 0% | 0% | 0% | 0% | 0% | 0% |

## Privacy Provisions: Handling Consents and Requests

The accounting for disclosures requirement is seen as difficult and is one most often mentioned as needing modification. AHIMA has sought such an amendment from the National Committee on Vital and Health Statistics, as have others, but to date no change has been recommended. The survey asked facilities to indicate **how many requests for an accounting** they have received.

Most commonly, respondents had received no or only a few requests for an accounting (67 percent of all respondents reported receiving no requests). Larger facilities were more likely to report more than 15 requests in the past 12 months. The high percentage of no requests would seem to underline the inefficient aspects of this requirement, especially since many of the disclosures may be the result of state laws and would normally be expected during the process of receiving healthcare services. AHIMA has recommended that the disclosure requirement be replaced in part by amending the notice of privacy practices to alert patients to disclosures required by law. With such a change, the number of disclosures requiring tracking would be limited and easier to facilitate within various organizations.

HIPAA provides facilities the option as to whether or not to **obtain patient consents for disclosures of information for treatment, payment, and healthcare operations** unless required by the state. The survey asked respondents if their state requires consent for disclosure for TPO purposes; responses were mixed. It appears that such state requirements may still be misunderstood by facilities, which is an opportunity for education.

The survey also asked facilities whether they required consents for TPO, as many facilities had previously indicated they wanted to keep such a consent (even though it is not required by HIPAA and may or may not be required by states). The percentage of H&HS facilities requiring TPO consents has dropped since 2004, but only slightly. Reports from privacy officers indicate that this may have been done in the name of administrative simplification.

| Require Consent for TPO (H&HS) | 2004 | 2005 |
|---|---|---|
| Yes | 51.5% | 48.2% |
| No | 46.5% | 50.5% |
| No Response | 2% | 1.3% |

The HIPAA regulation highlighted an individual's right to **request an amendment or correction** to their healthcare record. This provision received a considerable amount of attention in the media and initially caused providers concern, especially as an individual's understanding of what it meant to amend or correct a record was probably different from what the requirement demanded. The survey asked responders what percent of patients has actually requested information on amendment and correction. The largest percentage (60 percent) of total respondents reported that between 1 and 10 percent of patients had requested this information. (Smaller facilities were more likely to report no requests for this information.)

HIPAA also alerted patients of their rights to obtain a copy of their health record or information, and this provision also received media attention. The survey asked **how many patients had requested**

**copies of their health information**. The results are unclear; patients are requesting their records, but it is hard to tell if this is attributable to HIPAA.

| Request for Health Info. Record | >50,000 A/D | 20,000-49,999 A/D | 10,000-19,999 A/D | 5,000-9,999 A/D | 2,000-4,999 A/D | <2,000 A/D |
|---|---|---|---|---|---|---|
| None | 0% | 0% | 1.3% | 2.1% | 2.1% | 2% |
| 1-10% of patients | 23.3% | 28.9% | 25.3% | 22.9% | 25% | 53.3% |
| 11-20% | 20.9% | 23.3% | 27.8% | 25% | 28.1% | 21.1% |
| 21-30% | 14% | 19.8% | 20.3% | 17.7% | 13.5% | 9.9% |
| 31-50% | 23.3% | 13.3% | 17.7% | 19.8% | 17.7% | 11.2% |
| More than 50% | 18.6% | 16.7% | 7.6% | 12.5% | 13.5% | 2.6% |

Seventy-six percent of total respondents say they **charge patients for copies of health information**. Sixty-three percent charge between $0 and $5 per page; few charge more, although a number of respondents answered "other" indicating that they may have a different charging scheme. Charges vary considerably, as a number of states have regulations related to how much an institution can charge for such services and in some states hospitals can only charge for the actual copying, not for any clerical activities. With the advent of electronic health records and the concept of personal health records, the entire process is likely to change.

## Security: The Next Challenge

The HIPAA security rule emerges as the next challenge. With most hospitals set to implement the security regulation on April 21, 2005, the survey asked a number of questions related to security and the implementation process.

As in 2004, the survey asked if the facility had **designated a security officer**. The H&HS response showed an increase in security officers over 2004:

| Security Officer | 2004 | 2005 |
|---|---|---|
| Yes | 80% | 88.6% |
| No | 20% | 11.4% |

Many institutions see security as an information technology (IT) function and may have given the responsibility for implementation of the security to their IT department and not designated an individual as the officer. Whether or not this will work as an IT project remains to be seen, as the US Department of Health and Human Services requirements go beyond the IT function and require institutions to consider some non-computerized solutions. The survey data does not relate responses to this question to the question on whether a committee or task force exists.

**Forty-two percent of responders say the role of a security officer is a full-time one; 57 percent say it is part time**. The responses may depend in part on whether the facility sees the role as part of an existing IT effort or part of the facility's privacy responsibility. Among H&HS respondents, larger institutions were more likely to designate a full-time position for at least the implementation of the security rule, as they generally have more complicated systems to maintain and ensure compliance with a larger and diverse employee base.

| Full or Part Time | >50,000 A/D | 20,000-49,999 A/D | 10,000-19,999 A/D | 5,000-9,999 A/D | 2,000-4,999 A/D | <2,000 A/D |
|---|---|---|---|---|---|---|
| Full-time | 55% | 26.4% | 53.8% | 41.6% | 36.4% | 25.8% |
| Part-time | 45% | 73.6% | 46.3% | 58.4% | 63.6% | 74.2% |

Of those with a full-time security officer, H&HS respondents reported that an IS/IT employee was **most likely to fill the role**. HIM professionals are the second most likely group.

| Filling the Security Officer Role | 2004 | 2005 |
|---|---|---|
| HIM/Medical record dir/mgr | 5.6% | 9% |
| Compliance officer | 6.8% | 6.1% |
| Risk manager | 3% | 2.3% |
| Privacy officer | 7.2% | 4.3% |
| CIO | 8.9% | 7.9% |
| IS/IT personnel – dir/mgr | 59.9% | 60.9% |
| Other | 8.7% | 9.5% |

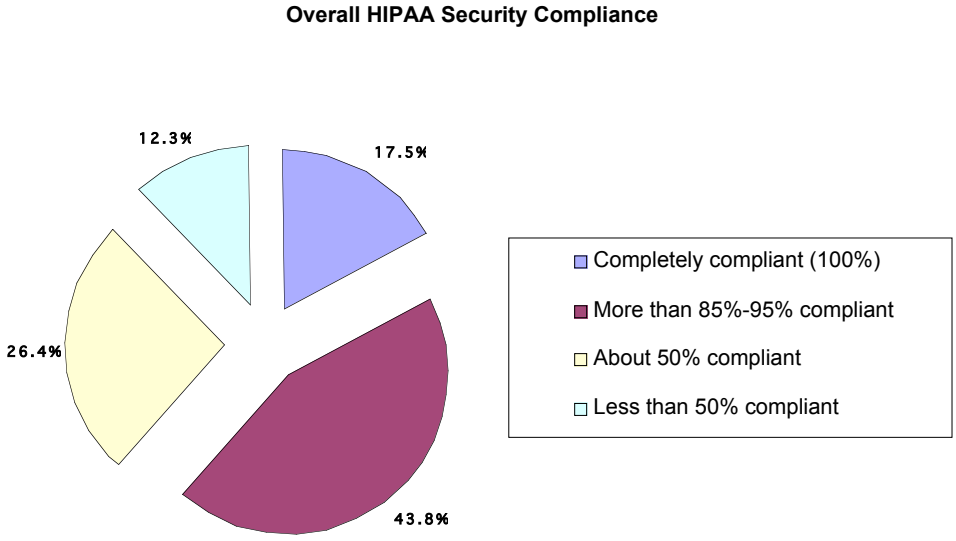
The relatively high number of "other" responses reflects small institutions' need to share the load among administrators and individuals with skills in organization, auditing, and so forth. We expect to see a shift in this make-up after the security rule is in place, because it would be unusual to see individuals in senior management positions dealing with day-to-day aspects of the rule. AHIMA is pleased to see that HIM professionals and privacy officers were recognized as having the skill necessary to facilitate and coordinate the security portion of the HIPAA rule.

A substantial number of H&HS respondents say their facilities have a **committee or task force related to security**, although there is a slight decrease from 2004. Not surprisingly, larger organizations were somewhat more likely to have committees in place than smaller ones.

| Task Force or Committee | 2004 | 2005 |
|---|---|---|
| Yes | 85.7% | 78.7% |
| No | 14.3% | 21.3% |

Several respondents pointed out that some organizations chose to use an existing committee–privacy or IT, for instance–rather than form a separate group. It was also suggested that some committees were formed to handle the initial steps in the security process and then disbanded to allow the IT department and others to carry out the necessary implementation.

Do facilities believe they are **compliant with HIPAA security**? The survey was completed in January 2005, when many organizations were still working toward meeting the April deadline. At that time, 17 percent of all responders described themselves as "completely compliant," 43 percent described themselves as 85 to 95 percent compliant, 26 percent felt they were about 50 percent compliant, and 12 percent felt they were less than 50 percent compliant.




The H&HS results are also roughly consistent with facility size:

| **Compliance with Security Rule** | **>50,000 A/D** | **20,000-49,999 A/D** | **10,000-19,999 A/D** | **5,000-9,999 A/D** | **2,000-4,999 A/D** | **<2,000 A/D** |
|---|---|---|---|---|---|---|
| Completely compliant (95-100%) | 17.8% | 13.8% | 12.4% | 12.5% | 21.6% | 18.1% |
| About 85-95% compliant | 53.3% | 48% | 39.3% | 47.5% | 42.3% | 42.6% |
| About 50% compliant | 26.7% | 23.7% | 38.2% | 33.8% | 27.8% | 26.6% |
| Less than 50% compliant | 2.2% | 14.5% | 10.1% | 6.3% | 8.2% | 12.8% |

The significant number of organizations responding at 50 percent or less compliance is not surprising given that the survey was completed in January 2005. As with many IT projects, completion can come quickly. On the other hand, it was reassuring to see the high percentage of organizations already indicating compliance. Many of the security rule requirements are common-sense requirements for record protection, security, and information technology standards, and many organizations had taken some steps to implement them long before HIPAA.

Facilities that were not ready frequently pointed to a lack of resources and time. Larger facilities also indicated a conflict with other IT projects under way, including the implementation of electronic medical records, while other smaller organizations indicated delays due to readiness for Joint Commission visits, prolonged gap analysis, lack of a designated security officer, and budget constraints. Facilities that were part of larger systems indicated that they believed the corporation was handling the problem, not indicating when the change would come to the individual facility. It is important to remember that unlike privacy, security is essentially a staff issue and not one that will directly impact the patient during the implementation process and initial days of compliance.

As with implementation of the HIPAA privacy regulations, the work done on security has also helped 54 percent of the total responding organizations **uncover problems with business practices or procedures**. The H&HS breakdown shows:

| Practice or Procedure Improvement | >50,000 A/D | 20,000-49,999 A/D | 10,000-19,999 A/D | 5,000-9,999 A/D | 2,000-4,999 A/D | <2,000 A/D |
|---|---|---|---|---|---|---|
| Yes | 60.5% | 45.6% | 70.6% | 68.4% | 56% | 52.2% |
| No | 39.5% | 54.4% | 29.4% | 31.6% | 44% | 47.8% |

Respondents were asked to identify the **number one problem identified and corrected during the security implementation process**. Not surprisingly, many identified the top issue as access and the tracking of access. Other issues were the more technical aspects of security related to IT systems. Some, but not many, mentioned physical security issues, but not in significant enough numbers to determine a serious industry issue with implementation. A number of commentators pointed out that that they were in the midst of implementation and would be better able to answer the question after the April implementation date.

## Privacy and Security Training: A Key Factor

Training and education have been important concerns for privacy officers, so for benchmarking purposes the survey asked some questions related to training and HIPAA.

The survey asked how facilities are handling **privacy training for new employees**. Sixty-two percent of total respondents surveyed reported new employee privacy training being done in-house by the privacy or education officer. In-house and Web-based instruction topped the list in most H&HS facilities, except where the smallest facilities favored video instruction over the Web:

| New Employee Privacy Training | >50,000 A/D | 20,000-49,999 A/D | 10,000-19,999 A/D | 5,000-9,999 A/D | 2,000-4,999 A/D | <2,000 A/D |
|---|---|---|---|---|---|---|
| In-house instruction | 57.8% | 70.3% | 64.8% | 52.4% | 55% | 73.2% |
| Video instruction | 6.7% | 14.5% | 11% | 11.9% | 16.3% | 15.4% |
| Web-based instruction | 35.5% | 14.3% | 22% | 33.3% | 25.5% | 8.3% |
| Other | 0% | 0.6% | 2.2% | 2.4% | 3.1% | 3.1% |

For **ongoing training for current employees**, training methods varied considerably. Reminders and newsletter articles topped the list as ways to prompt employees to remember to continue their privacy vigilance.

HIPAA also requires **security training** for all personnel and volunteers. Forty-five percent of all respondents indicated that their facility had developed its own educational program for initial training. For the H&HS respondents, as with privacy training, online education was also popular. Other preferred methods varied with facility size.

| Security Training | >50,000 A/D | 20,000-49,999 A/D | 10,000-19,999 A/D | 5,000-9,999 A/D | 2,000-4,999 A/D | <2,000 A/D |
|---|---|---|---|---|---|---|
| Outsourced professional program | 2.4% | 2.2% | 0% | 5.1% | 2.3% | 2% |
| Facility-developed program | 35.7% | 54.8% | 41.1% | 43% | 50% | 45% |
| Videotape presentation | 7.1% | 10.8% | 7.8% | 7.6% | 3.5% | 10.6% |
| Knowledge and skill level testing | 0% | 3.2% | 1.1% | 1.3% | 2.3% | 0.7% |
| Online education program | 31% | 4.3% | 12.2% | 11.4% | 14% | 9.3% |
| Interactive software tool | 2.4% | 1.1% | 5.6% | 11.4% | 1.2% | 1.3% |

| | | | | | | |
|---|---|---|---|---|---|---|
| Signed confidentiality statement | 14.3% | 7.5% | 8.9% | 3.8% | 9.3% | 15.9% |
| Group discussion and interaction | 2.4% | 3.2% | 2.2% | 1.3% | 1.2% | 3.3% |
| HIPAA compliance hotline | 0% | 0% | 1.1% | 1.3% | 1.2% | 0% |
| Other | 4.8% | 12.9% | 20% | 13.9% | 15.1% | 11.9% |

## Information on the Go: Outsourcing

Outsourcing has become a hot topic in many industries and healthcare is no exception. In 2004, outsourcing became a topic of debate (and, at times, legislation) as fears grew that it could compromise the confidentiality of personal health information. The survey asked some questions related to outsourcing to highlight the need to protect personal health information, wherever it may go. While not a definitive snapshot of all healthcare outsourcing, the results point to issues that could arise in any future networking of health information.

The survey asked whether facilities **outsource any health information management functions**. While 42 percent of the total respondents answered yes, the H&HS results vary across facility size.

| **Outsource Any HIM Functions?** | **>50,000 A/D** | **20,000-49,999 A/D** | **10,000-19,999 A/D** | **5,000-9,999 A/D** | **2,000-4,999 A/D** | **<2,000 A/D** |
|---|---|---|---|---|---|---|
| Yes | 64.4% | 41.1% | 62.2% | 64.3% | 68.1% | 35.1% |
| No | 35.6% | 58.9% | 37.8% | 35.7% | 31.9% | 64.9% |

More research needs to be done on this issue to determine the causes for variation in some categories.

Transcription and release of information were the two **most frequently outsourced HIM functions**. The survey did not ask whether these functions were outsourced to companies out of state, out of the country, or just out of the facility. Again, H&HS results vary with facility size.

| **Functions Outsourced** | **>50,000 A/D** | **20,000-49,999 A/D** | **10,000-19,999 A/D** | **5,000-9,999 A/D** | **2,000-4,999 A/D** | **<2,000 A/D** |
|---|---|---|---|---|---|---|
| Transcription | 86.7% | 76.2% | 74.6% | 68.9% | 82.4% | 72.9% |
| Coding | 30% | 19% | 28.4% | 21.3% | 25% | 23.7% |
| Release of information | 76.7% | 50% | 64.2% | 72.1% | 39.1% | 35.6% |
| Other | 6.7% | 4.8% | 9% | 11.5% | 10.3% | 13.6% |

Outsourcing of personal health information requires a business associate contract, according to HIPAA. However, some outsourcing vendors in turn outsource their business. The survey asked whether facilities' **business associate contracts address the use of subcontractors**. While many H&HS responders answered yes, in some categories a significant percentage of them were not sure.

| **BAC Addresses Use of Subcontractors** | **>50,000 A/D** | **20,000-49,999 A/D** | **10,000-19,999 A/D** | **5,000-9,999 A/D** | **2,000-4,999 A/D** | **<2,000 A/D** |
|---|---|---|---|---|---|---|
| Yes | 86.7% | 74% | 78.4% | 78.6% | 80.2% | 53.9% |
| No | 4.4% | 4.2% | 3.1% | 9.5% | 4.4% | 7.8% |
| Not sure | 8.9% | 21.9% | 18.6% | 11.9% | 15.4% | 38.3% |

Finally, the survey asked whether business associate contracts address the outsourcing of health information to offshore affiliates or companies. Again, H&HS responses varied, indicating that this issue is probably not yet a closed case for the industry.

| BAC Addresses Outsourcing | >50,000 A/D | 20,000-49,999 A/D | 10,000-19,999 A/D | 5,000-9,999 A/D | 2,000-4,999 A/D | <2,000 A/D |
|---|---|---|---|---|---|---|
| Yes | 47.7% | 20.8% | 29.9% | 29.8% | 28.6% | 20.1% |
| No | 36.4% | 45.8% | 40.2% | 44% | 44% | 46.1% |
| Not sure | 15.9% | 33.3% | 29.9% | 26.2% | 27.5% | 33.8% |

# Conclusion

Two years after the implementation of the HIPAA privacy rule, the AHIMA survey finds the following conclusions:

- **The majority of facilities are significantly compliant with privacy and expected to be compliant with HIPAA security** as well. The responses, however, indicate that privacy officers want the industry to know that resources are needed to maintain compliance.
- While facilities may expect to be "done" with HIPAA, privacy officers understand the **need for renewed commitment to education and training for ongoing success**. Again, the respondents believe that privacy compliance is the duty of everyone in an organization, not just those charged with overseeing the process.
- Most respondents have had little or no difficulty implementing provisions of the privacy rule, but reports of difficulties with a handful of requirements suggest **areas where more education or refinement may be necessary**. Certain areas continue to present operational challenges, such as:
    - -Accounting for disclosures
    - -Access and release of information to law enforcement
    - -Access and release of information to relatives or patients' "significant others"
    - -Release of information for research protocols
    - -Access and release of information for subpoenas versus court orders
    - -Business associate agreements.
- **Protecting personal health information continues to be an important goal**, as emerging issues such as outsourcing suggest.

While HIPAA implementation has compelled organizations to make strides in the area of privacy and security, more challenges are ahead. Privacy officers soon will be faced with the advent of regional and national health information exchanges. Even small indicators of privacy or security noncompliance must be addressed so that privacy issues do not challenge the movement to develop regional and national health information networks.

Privacy officers are concerned that the public, the health professionals they deal with, and others in these new arenas must be actively educated and committed to the privacy, confidentiality, and security necessary to build the public's trust. AHIMA hopes that the information in this survey will help organizations examine where they stand with regard to the obligations of privacy and security. It also hopes this information will help the industry understand where it needs to go to build a national health information infrastructure that provides patients with trustworthy confidentiality.