



The State of HIPAA Privacy and Security Compliance

April 2006



A Report by the American Health Information Management Association

Contents

Executive Summary	3
Survey Results and Analysis	5
Conclusion	20

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:

Jill Callahan Dennis, JD, RHIA

Meg Featheringham

Susan Fenton, MBA, RHIA

Sue Fiorio

Kevin Gould

Scott Mackenzie

Cindy Nichols, RHIA, CHP

Mark Piszczor

Dan Rode, MBA, FHFMA

Anne Zender, MA

American Health Information Management Association

233 N. Michigan Ave., 21st Floor

Chicago, IL 60601-5800

www.ahima.org

© 2006

Executive Summary

About the 2006 Survey

For the past three years, the American Health Information Management Association (AHIMA) has surveyed healthcare privacy officers and others whose jobs relate to the HIPAA privacy function to gain an understanding of where healthcare organizations stand with regard to implementing the privacy and security rules of the Health Insurance Portability and Accountability Act (HIPAA). The first survey results were released in April 2004, one year after the implementation of the final privacy rule. In 2005, the second annual survey looked at compliance with the privacy rule and the security rule, which went into effect on April 21, 2005.

This third annual survey revisits these areas to assess how well the industry is maintaining HIPAA privacy and security compliance as a part of the normal course of business as it moves further away from the implementation deadlines.

AHIMA intends the results of the survey will reinforce the importance of protecting the privacy, confidentiality, and security of personal health information. It also intends to help the industry understand the most difficult areas of privacy and security implementation that may need more study.

Sixty-four percent of respondents to the 2006 survey work in a hospital setting and the remaining 36 percent in integrated healthcare delivery systems. Of the 1,117 survey respondents, 40 percent are designated privacy or security officers, with another 9 percent functioning as the privacy or security officer without the official title. Thirty-two percent indicated they serve on HIPAA privacy or security teams or committees.

Findings

The majority of facilities continue to be essentially compliant with HIPAA privacy and security regulations. Nearly 39 percent of hospitals and health systems report full privacy compliance, holding steady with last year's 40 percent and a considerable increase over 2004's 23 percent. Unfortunately, the number of those who believe that they are more than 85 percent compliant with the privacy regulations has dropped in the last year. The percentage of respondents who believed their institution was more than 85 percent compliant dropped to 85 percent in 2006, down from 91 percent in 2005. As a result, the percent of respondents who believed they were less than 85 percent compliant increased from 9 percent in 2005 to 15 percent in 2006.

Responses to other questions give insight into this slight decrease and show that while it is not a significant change, it is enough to raise concern. For example, **fifty-five percent of respondents indicated that resources are their most significant barrier to full privacy compliance.** Privacy officers particularly need support for education and training of new staff, while a lack of resources and competing priorities have led some hospital and health system staff to slack off regarding all aspects of the privacy rule. The issue of budget also appears to impact the level of privacy training and monitoring that a privacy officer or staff are capable of providing. Finally, privacy officers report sensing a loss of support from senior management, both in ensuring the facility staff is aware of the need for privacy as well as ensuring sufficient budgeting for education.

After three years, most providers are growing accustomed to the various provisions of the privacy rule, but there are still reports of **difficulties with a select few requirements, notably accounting for disclosures.** Not surprisingly, many respondents would like to see changes in the accounting for disclosures provision of the privacy rule. This is especially true where the demand for such accounting is extremely low. Most commonly, respondents had received only a few requests for an accounting or none at all (64 percent of all respondents reported receiving no requests). For many, this provision is not only burdensome but also significantly inefficient.

One year into the HIPAA security regulations, **a quarter of the surveyed facilities indicate compliance at the top level with another 50 percent indicating that they are close to full compliance.** This represents an increase over 2005, when 17 percent of all respondents described themselves as "completely compliant," and 43

percent described themselves as 85 to 95 percent compliant. It appears that the security regulations were much easier to achieve than the privacy rules.

Some **consumers are becoming more aware of the importance of the privacy of health information**, as evidenced by the increased number of questions providers report being asked by patients. More disturbingly, 22 percent reported encountering consumers who refused to sign release of information forms. More research is needed to understand how deep those fears are or what consumers are most worried about. Clearly the industry now has an opportunity to educate consumers on how their personal health information will (or should be) protected. This is an important step. Without consumer confidence the national health information network will never succeed.

Just under a third (31 percent) of respondents indicated that they were currently involved in a local or regional health information exchange project. For those involved in health information exchanges, it appears that HIM professionals are addressing release of information, privacy, and security areas, with authentication being one of the main security issues being investigated.

Conclusion

Three years after the implementation of the HIPAA privacy rule, the AHIMA survey concludes the following:

HIPAA implementation has been a challenge for organizations, and it appears that for the majority the challenge has been met. However, the need for privacy, confidentiality, and security remain, especially as organizations tighten staffing and budgets. A slight drop in the number of facilities reporting themselves to be fully or mostly compliant with HIPAA should serve as a warning to the industry that compliance should not be taken for granted.

If the support for privacy and security and the need for ongoing training are not maintained (and, in a few areas, increased), all the work that has been put into the HIPAA compliance efforts of the last few years may be undone over time.

The need for support of privacy and security must also reach beyond facilities. The federal government's approach to HIPAA enforcement has been to educate rather than fine or prosecute offenders. While we applaud this approach, a concerted effort to educate and remind the healthcare industry and others of the need to maintain and continually improve privacy efforts is equally needed.

The healthcare industry has much to learn from the lessons of HIPAA as it moves toward electronic health records and a nationwide health information network. There is considerable disagreement on whether electronic health records will improve privacy or security and there are many concerns on how information networks will protect data. Consumers will be watching the healthcare industry to see how well it complies with the HIPAA rules before they put their trust in a national health information exchange. Communicating with consumers, answering their questions and addressing their concerns, may be a key to advancing health information exchange activities. Privacy officers and HIM professionals will be important partners in this process. AHIMA believes that the time is right for an open dialogue about the value of privacy and security at both the national and organizational levels.

Survey Results and Analysis

About the 2006 Survey

For the past three years, the American Health Information Management Association (AHIMA) has surveyed healthcare privacy officers and others whose jobs relate to the HIPAA privacy function to gain an understanding of where healthcare organizations stand with regard to implementing the privacy and security rules of the Health Insurance Portability and Accountability Act (HIPAA). The first survey results were released in April 2004, one year after the implementation of the final privacy rule. In 2005, the second annual survey looked at compliance with the privacy rule and the security rule, which went into effect on April 21, 2005.

This third annual survey revisits these areas to assess how well the industry is maintaining HIPAA privacy and security compliance as a part of the normal course of business as it moves further away from the implementation deadlines.

AHIMA intends the results of the survey will reinforce the importance of protecting the privacy, confidentiality, and security of personal health information. It also intends to help the industry understand the most areas of privacy and security implementation that may need more study. The findings are particularly significant in light of the research currently being conducted by the Health Information Security and Privacy Collaboration (HISPC) at the behest of the Office of the National Coordinator for Health Information Technology (ONC). HISPC is working with state governments to assess and develop plans to address variations in policies and business practices that affect privacy and security. The goal is to address barriers to interoperable health information exchange.

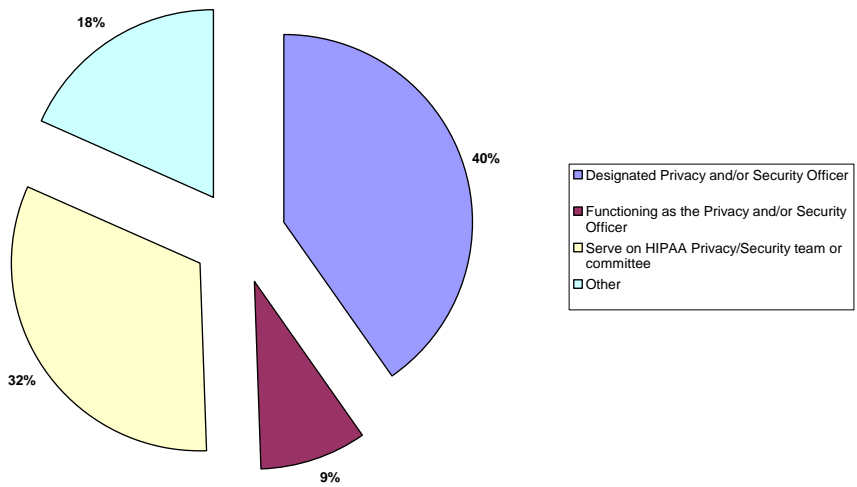
AHIMA conducted the survey in January 2006, with the assistance of an impartial third-party market research firm. E-mail invitations were sent to AHIMA members who were considered most likely to have participated significantly in the HIPAA implementation process and others who had participated in various HIPAA-related educational opportunities provided by AHIMA. The survey received 1,117 qualified responses.

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 AHIMA seeks to educate the public and the industry on issues related to HIPAA privacy and security 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 1,117 respondents, 40 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. Thirty-two percent indicated that they served on a HIPAA privacy or security team or committee while 18 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 the area. It appears, therefore, that 49 percent of all respondents were directly involved in the privacy or security functions of their organization.

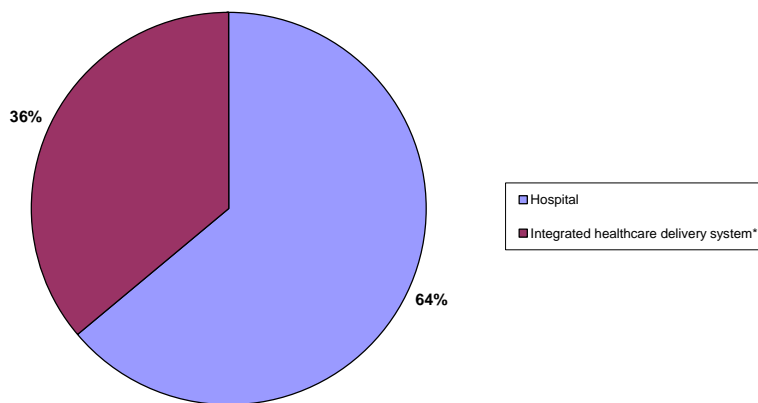


Types of Facilities

In 2006, 64 percent of survey respondents said they work in a hospital setting; the remaining 36 percent work in integrated healthcare delivery systems. For the purposes of this survey, respondents are categorized by numbers of admissions/discharges (A/D) during the last calendar year (as reported by the respondents). The categories are:

- More than 50,000 A/D (5 percent of respondents)
- 20,000-49,999 A/D (10 percent)
- 10,000-19,999 A/D (13 percent)
- 5,000-9,999 A/D (21 percent)
- 2,000-4,999 A/D (22 percent)
- Fewer than 2,000 A/D (28 percent)

Hospitals and Health Systems



Privacy: Who's in Charge?

When asked **whether their facility has a privacy officer**, 27 percent of all respondents had a full-time officer, while 61 percent had a part-time officer. Consistent with other years, this survey finds that 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.

	>50,000 A/D	20,000- 49,999 A/D	100,000- 19,999 A/D	5,000- 9,999 A/D	2,000- 4,999 A/D	<2,000 A/D
Privacy Officer						
Full time	52.5%	46.8%	26.2%	21.7%	18.4%	28.6%
Part time	47.4%	53.1%	72.4%	75.4%	78.0%	70.1%
None	.1%	0.1%	1.4%	2.9%	3.6%	1.3%

Even then, however, the largest reporting group indicates only 52 percent have a full-time officer, while in the smallest group almost 30 percent have a full-time privacy officer. Privacy officer employment levels seem to be stable. A large majority of total respondents (85 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 (2 percent) still report having no privacy officer at all. Nine percent say they do not know—a 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 61 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 26 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**. Sixty-four percent of respondents said that they did, a 17 percent drop since 2005, and a 25 percent drop since 2004. Eighty-eight percent of facilities with the highest number of admissions/discharges reported having such a committee.

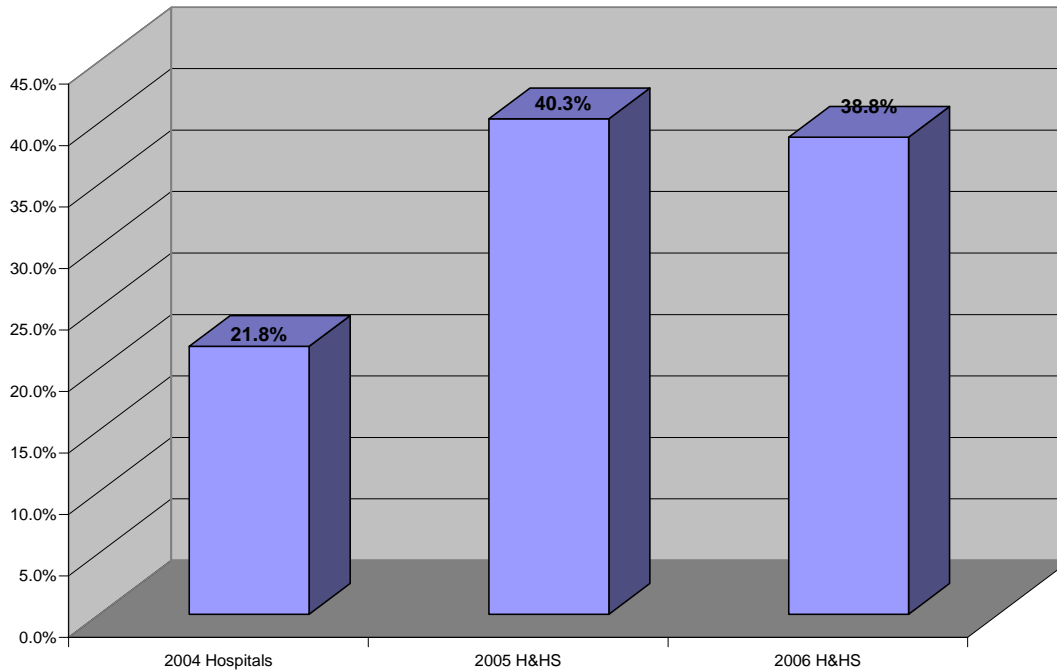
In written comments, many respondents noted a lack of resources (time, education budget, and in some cases staff) to complete what they now view as additional duties associated with the privacy rule. Respondents reported that employment shortages resulting in a busier work force and higher staff turnover add a burden to educate new employees and keep up education and reminders for existing staff. Similarly, for a second year, many felt that their lack of time and to some extent resources could mean that their institution's commitment to the privacy compliance process has diminished.

Privacy: How Compliant Are We?

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

In 2006, 39 percent of respondents reported that they were fully compliant, compared to 40 percent in 2005 and 23 percent in 2004. While the difference between 2005 and 2006 is not statistically significant, a larger drop is seen in the number of respondents reporting that they were 85 percent compliant. Overall, 85 percent of all respondents reported being 85 percent or more compliant this year, compared to 91 percent in 2005. As a result, the percent of respondents who believed they were less than 85 percent compliant increased from 9 percent in 2005 to 15 percent in 2006. This drop in perceived levels of compliance is spread across organizations of all sizes and appears to correspond with many comments indicating that some organizations' emphasis on and support for HIPAA privacy programs has diminished. Respondents report needing more staff, time, ongoing education programs, and support from organization administrators and medical staff leadership.

Full Privacy Compliance



Two years after the compliance deadline for hospitals and health plans, only 1 percent of respondents indicate that they are less than 50 percent compliant. In 2005, 4 percent of respondents indicated they were less than 50 percent compliant, compared to 7 percent in 2004.

2006 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	Total
Less than 50%	5.1%	0.0%	0.7%	0.4%	0.8%	1.3%	1.0%
About 50%-85%	15.3%	9.2%	14.5%	12.1%	11.6%	18.2%	13.9%
> 85%	79.7%	90.8%	84.8%	87.6%	87.69%	80.5%	85.2%

Difficulties with HIPAA Privacy Requirements

The survey asked whether respondents were having difficulties implementing and enforcing specific provisions of the privacy rule. As in 2005, most respondents reported no or only slight difficulties with most of the requirements. However, in some areas respondents reported moderate or extreme difficulties.

Under HIPAA, individuals have the right to ask for an **accounting of all disclosures of protected health information** for purposes other than treatment, payment, or healthcare operations. As found in previous surveys, this requirement was the most significant issue for respondents, with 15 percent indicating that it was moderately to extremely difficult. Although AHIMA, the American Hospital Association, and others have asked for changes to this requirement, none are expected in the near future. In 2006, larger organizations most frequently report difficulty with this requirement.

Difficulty Accounting	>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	<2000 A/D	Total
None	45.8%	49.5%	39.3%	39.6%	46.4%	49.7%	45.2%
Slight	30.5%	31.2%	46.9%	44.6%	41.6%	36.6%	39.9%
Moderate	13.6%	13.8%	11.0%	12.5%	10.8%	9.2%	11.2%
Extreme	10.2%	5.5%	2.8%	3.3%	1.2%	4.5%	3.7%

Ten percent of respondents identified **confusion by individuals/patients in understanding the notice of privacy practices** as a problem. Such recognition of patient confusion might also be the reason more than 55 percent of respondents say they have changed their notice (see page 13).

Confusion Understanding Notice	>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	<2000 A/D
None	50.8%	48.6%	57.2%	62.9%	60.8%	55.1%
Slight	37.3%	39.4%	31.0%	28.8%	27.2%	37.3%
Moderate	11.9%	11.9%	9.7%	7.1%	10.0%	5.4%
Extreme	0.0%	0.0%	2.1%	1.3%	2.0%	2.2%

In 2006, 10 percent of respondents reported difficulty **obtaining protected health information from other providers**. Anecdotes indicate that the problem may be particularly acute for schools (because of conflicting state and federal Department of Education laws and regulations) and for individual practices that do not understand their options under HIPAA. This is an area where the Office of the National Coordinator on Health Information Technology's study on privacy may be able to shed additional light.

Difficulty Obtaining	>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	Total
None	59.3%	50.5%	49.7%	45.0%	42.0%	47.5%	46.9%
Slight	35.6%	39.4%	40.7%	45.4%	49.2%	41.4%	43.4%
Moderate	5.1%	9.2%	9.7%	7.5%	8.4%	8.3%	8.2%
Extreme	0.0%	0.9%	0.0%	2.1%	0.4%	2.9%	1.4%

Access and release of information to patients' relatives or significant others is a problem for 9 percent of the respondents. The reasons why are numerous. Respondents note that identifying a patient's personal representative can be complex, as can various laws associated with durable power of attorney. Others note that getting patients, relatives or significant others, institutions, and laws to all agree is often difficult.

Difficulty Relatives	>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	Total
None	40.7%	38.5%	35.9%	44.2%	36.8%	39.8%	39.5%
Slight	54.2%	50.5%	55.9%	47.1%	57.6%	47.1%	51.3%
Moderate	5.1%	9.2%	8.3%	7.1%	4.4%	10.5%	7.7%
Extreme	0.0%	1.8%	0.0%	1.7%	1.2%	2.5%	1.5%

It appears that even after three years, **business associate agreements** continue to cause difficulty for healthcare providers. Nine percent of respondents indicated moderate to extreme difficulty with this requirement. As noted in previous surveys, larger providers likely have more potential business associate agreements, leading to problems of volume as well as complexity. Smaller facilities may have fewer business associate agreements but have also fewer staff and less time to manage and monitor these agreements.

Difficulty Bus. Assoc.	>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	Total
None	64.4%	54.1%	43.4%	44.6%	45.6%	50.3%	48.3%
Slight	35.4%	35.8%	46.2%	48.3%	47.2%	40.1%	43.1%
Moderate	10.2%	10.1%	9.7%	5.8%	6.0%	7.6%	7.5%
Extreme	0.0%	0.0%	0.7%	1.3%	1.2%	1.9%	1.2%

Access and release of information to law enforcement was identified as a problem by 8 percent of respondents. We know from a variety of discussions that multiple jurisdictions, including state and federal, remain problems along with the need to educate law enforcement about HIPAA and state and local restrictions. This area could benefit from HISPC's study.

Difficulty Law	>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	Total
None	50.8%	52.3%	54.5%	55.8%	52.4%	58.9%	55.1%
Slight	37.3%	37.6%	41.4%	36.7%	38.4%	32.8%	36.7%
Moderate	10.2%	8.3%	3.4%	6.7%	8.0%	6.7%	6.9%
Extreme	1.7%	1.8%	0.7%	0.8%	1.2%	1.6%	1.3%

Seven percent of respondents indicated moderate to extreme difficulty with **access and release of information for subpoenas versus court orders**. We noted in 2005 that many problems with subpoenas and court orders occur because attorneys and courts continue to be unaware of HIPAA regulations or rely on state rules inappropriately. This may indicate that other professions, such as law enforcement, appear to be paying less attention to HIPAA, especially in locations where HIPAA education for non-healthcare entities was not available.

Difficulty Court	>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	Total
None	52.5%	60.6%	59.3%	56.3%	55.6%	64.0%	58.9%
Slight	37.3%	30.3%	33.8%	37.1%	36.4%	29.6%	33.8%
Moderate	8.5%	8.3%	6.9%	5.8%	8.0%	5.1%	6.6%
Extreme	1.7%	0.9%	0.0%	0.8%	0.0%	1.3%	0.7%

Confusion related to **information being released for research protocols** continues. It is clear this issue has not been resolved at a federal level between human subject protection regulations and HIPAA. While overall 5 percent of respondents indicated moderate to extreme difficulty with the requirement, most of the difficulties exist in larger institutions where more research occurs. However, respondents from the largest organizations may report fewer difficulties than the next largest group because most large teaching-tertiary facilities and systems have specific staff managing research protocols.

Difficulty Research	>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	Total
None	61.0%	53.2%	50.3%	53.8%	59.2%	69.4%	59.3%
Slight	30.5%	37.6%	41.4%	41.7%	36.0%	27.1%	35.3%
Moderate	8.5%	9.2%	7.6%	3.3%	3.6%	3.2%	4.7%
Extreme	0.0%	0.0%	0.7%	1.3%	1.2%	0.3%	0.7%

The survey asked, "**Which areas of the HIPAA privacy rule do you believe need to be modified by the federal government?**" 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 (29 percent)
- Access and release of information to relatives or significant others (20 percent)
- Post-care disclosure to patients (16 percent)
- Release of information to law enforcement (16 percent)
- Subpoenas and court orders (15 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
Accounting for disclosure	47.5%	41.3%	34.0%	23.8%	23.7%	29.0%
Access to relatives	8.5%	16.5%	25.0%	18.8%	20.9%	22.9%
Post-care disclosure to patients	8.5%	9.2%	14.6%	22.6%	18.5%	15.6%
Disclosure to law enforcement	11.9%	15.6%	16.0%	19.7%	18.9%	12.4%
Subpoenas and court orders	11.9%	17.4%	15.3%	17.6%	16.9%	12.1%

As in previous years, accounting for disclosures remains a top issue for all organizations. It must again be noted that the data show that the number of requests for an accounting is very small (see page 14), but responding to any requests requires a considerable amount of administrative work.

Other Privacy Concerns

The survey asked respondents to identify the number one barrier to their facility's ability to be in full compliance with the HIPAA privacy requirements. Resources topped the list from 55 percent of respondents, with 24 percent citing administrative support and 6 percent citing state preemption situations. The remaining 10 percent appeared to have responses that could be easily categorized into the resource and support categories. Only 3 percent of respondents indicated that there were no barriers at present.

As AHIMA noted in its 2005 report, the need for resources and support is increasingly mentioned. Resources are often translated into more staff or more time for privacy activities, including monitoring and correcting problems. Education remains a top priority, and many report the challenge of expanding education of new employees and retraining existing employees with limited resources.

Administrative support goes hand in hand with this issue. Without significant support, privacy officers or committees have difficulties securing budget or resources to achieve full compliance. Administrative support either from executives or clinical leadership is also directly tied to the attitude employees take toward promoting and incorporating privacy practices in their daily functions. Without this support, reports of slippage in daily practices may grow more prevalent.

Since the implementation of the privacy rule in 2003, the number of external or nationwide educational programs on privacy has reduced significantly. Emphasis on the need for good privacy practices has also decreased, so it is possible that administrators or clinical leaders believe maintaining and improving privacy practices is less of a priority. From comments made by the respondents, it appears that many privacy officers are doing their best, but their calls for more support and resources are going unheard. This may be why organizations report feeling that they are less compliant than they were.

The Impact of State Pre-emption

The 2006 data show a small decrease in the number of respondents who say that the impact of the HIPAA allowance for **state pre-emption** has caused difficulties, as indicated by 22 percent of the respondents, compared to 25 percent in 2005. 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, and it will certainly be of interest to HISPC.

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 respondents were:

- Release of information to relatives or significant others (28 percent)

- Release of information to law enforcement (27 percent)
- Release pursuant to subpoena/court order (26 percent)
- Release related to state requirements for consents (25 percent)
- Release of information to patients (22 percent)

As time goes by, it may be that providers are reporting fewer problems because they are more comfortable with the rules. Consent requirements have changed in some states, so differences with HIPAA may have been reduced. However, more than a quarter of respondents continue to experience difficulty in this area, and it continues to be a concern to many privacy groups seeking to remove the treatment, payment, and healthcare operations requirement from HIPAA. As noted in the 2005 survey results, about 50 percent of the states have a requirement for consent and many organizations have included consents even though they are optional under HIPAA. Issues with release of information to courts and law enforcement are no surprise since the conflicts in the state preemption often occur in these areas. Many state laws are written without considering exceptions for healthcare. Until conflicts in legal areas are examined and resolved (a subject for HISPC), problems will continue.

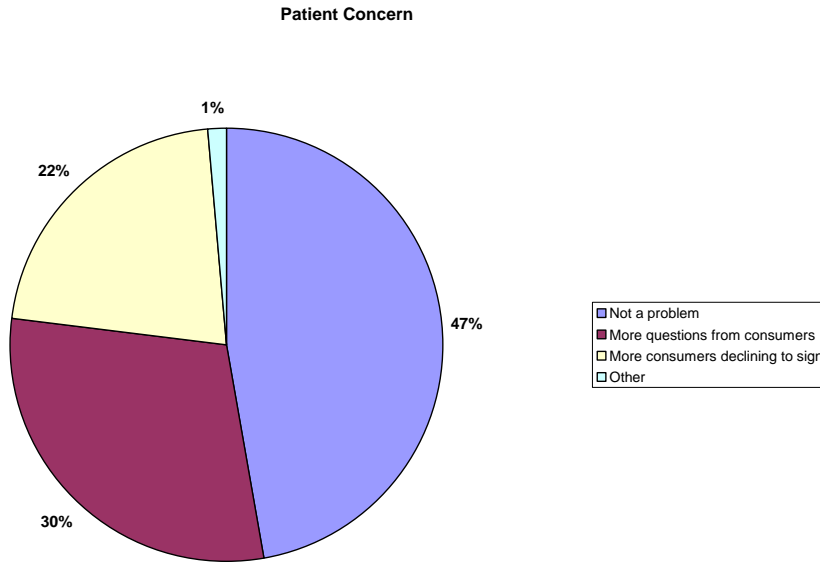
Pre-emption issues can also complicate release of information to patients and relatives. In 2005, providers in several states began to have problems charging for the cost of release of records. Part of this problem concerned states that have established rules with regard to who and what can be billed for this service. In several cases persons with a questionable relationship to the patient under HIPAA claimed they should not be charged because they were acting on behalf of the patients. This matter was recently resolved by the Office for Civil Rights, but it is too early to tell if there will be fewer problems associated with such releases. As mentioned in 2005, the identification of patient representatives also continues to create conflict between states and the HIPAA rules, and this may not be resolved until differences can be clearly defined.

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%	18.8%	19.0%	20.0%	23.5%	16.7%
Law enforcement	30.8%	62.5%	23.8%	22.9%	26.5%	20.0%
Subpoenas/court orders	30.8%	43.8%	14.3%	31.4%	20.6%	30.0%
Disclosure to relatives/significant others	23.1%	25.0%	33.3%	34.3%	17.6%	30.0%
Business associate agreements	23.1%	12.5%	19.0%	22.9%	8.8%	18.3%
Post-care release of information to patients/relatives	7.7%	25.0%	23.8%	14.3%	20.6%	18.3%

Reactions to HIPAA Privacy

How are **patients reacting to HIPAA privacy** efforts? The survey asked some new questions designed to gauge patient reaction.

Consumer groups and healthcare policy makers have devoted considerable attention to this question. This year the survey referred to a recent report that noted that a high percentage of patients were concerned about privacy of their health records and asked, “How has that manifested itself in your facility?” Forty-seven percent of respondents said it was “not a problem.” Another 30 percent said they had encountered more questions from consumers. More disturbingly, 22 percent reported encountering more consumers who refused to sign release of information forms.



While HIM professionals are pleased that patients are asking more questions, it is not clear why they are asking them. Questions may be resulting from concerns related to the notice of privacy practices or other forms or from misunderstanding privacy issues. The survey does not shed light on why some individuals refuse to sign forms. Larger facilities seem to report more questions from consumers, while those at smaller facilities seem more likely to say that privacy concerns are not a problem.

	>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	Total
More declining to sign	3.4%	16.5%	35.2%	27.5%	24.8%	13.7%	21.7%
More questions from consumers	54.2%	38.5%	24.1%	33.8%	26.8%	23.9%	29.7%
Not a problem	39.0%	43.1%	39.3%	37.5%	47.2%	61.1%	47.2%
Other	3.4%	1.9%	1.4%	1.2%	1.2%	1.3%	1.4%

Some consumers are becoming more aware of the importance of the privacy of health information. Certainly the increased discussion of electronic health records, a nationwide health information network, local networks, stolen or misplaced laptops, and identity theft are getting more attention and raising fears among some. It is not clear how deep those fears are or what consumers are most worried about. But clearly the industry now has an opportunity to educate consumers on how their personal health information will (or should) be protected as the health information environment changes. This is an important step. Without consumer confidence, the national health information network will never succeed.

More than 55 percent of all respondents indicate that their facilities have **changed their privacy notices** since April 2004, a considerable increase from 19 percent in 2005. 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.

Most of the changes were made to clarify language and make the notice easier to understand. Often changes were caused by state law changes, telephone numbers, title changes, and so forth. Facilities could eliminate some of these changes by providing titles rather than names on their privacy notices.

HIPAA requires facilities 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 (57 percent). A breakdown shows:

	>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
Complaints						
Yes	71.2%	65.1%	58.6%	62.9%	60.4%	44.3%
No	28.8%	34.9%	41.4%	37.1%	39.6%	55.7%

The survey asked whether respondents believed the difference between federal HIPAA requirements and state laws caused any complaints. Responses varied by size.

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	30.5%	36.7%	41.4%	37.5%	40.8%	56.1%
No	69.5%	63.3%	58.6%	62.5%	59.2%	43.9%

In general, 42 percent of respondents reported that their facility's staff was generally very supportive of initiatives related to patient privacy, with another 41 percent reporting staff were somewhat supportive. In 2006, 16 percent said that staff were indifferent or not supportive, compared to 18 percent in 2005.

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	67.8%	54.1%	51.7%	44.2%	42.8%	42.0%
Somewhat supportive	25.4%	35.8%	40.7%	45.0%	46.0%	41.1%
Indifferent	1.7%	10.1%	4.1%	7.1%	8.4%	13.4%
Not very supportive	5.1%	0.0%	2.1%	2.9%	1.6%	3.5%
Not at all supportive	0.0%	0.0%	1.4%	0.8%	1.2%	0.0%

Privacy Provisions: Handling Consents and Requests

As in previous years, the accounting for disclosures requirement is reported to be a difficult one and is most often mentioned as needing modification. AHIMA and other groups have sought a recommendation for such an amendment from the National Committee on Vital and Health Statistics and the Office for Civil Rights, but at this time no amendment is expected in the near future. The survey asked facilities to indicate **how many requests for an accounting** they have received in 2005 from all patients seen.

Number of Requests	Percent
0	63.7%
1-2	14.3%
3-4	4.8%
5-10	3.8%
11-15	2.1%
More than 15	2.4%
Do not know	8.9%

Most commonly, respondents had received only a few requests for an accounting or none at all (64 percent of all respondents reported receiving no requests). Of those reporting in total, only 2 percent of facilities report receiving a volume of more than 15, and when this is broken down by size only facilities with between 10,000 and 20,000

admissions reported a percentage higher (3 percent). Volume of requests varies widely among the range of respondents. AHIMA recommends that the disclosure requirement be replaced in part by amending the notice of privacy practices to alert patients to disclosures required by law. If such disclosures did not have to be included in an accounting (e.g., if patients were informed in the notice of the laws concerning such a release) it is likely the number of accountings for other purposes would go down.

Accounting for Disclosure Requests	>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
0	35.6%	41.3%	57.9%	65.8%	66.4%	75.7%
1-2	23.7%	28.4%	14.5%	17.1%	12.4%	7.0%
3-4	6.8%	7.3%	3.4%	4.2%	6.4%	3.5%
5-10	8.5%	3.7%	4.8%	3.8%	4.8%	1.9%
11-15	1.7%	1.8%	3.4%	2.5%	2.0%	1.3%
More than 15	1.7%	1.8%	5.5%	1.7%	0.8%	3.2%
Don't know	22.0%	15.6%	10.3%	5.0%	7.2%	7.6%

The HIPAA regulation highlighted an individual's right to **request an amendment or correction** to his or her healthcare record. The 2006 survey asked whether requests for amendment to the content of an individual's record had changed since April 14, 2003. Thirty-three percent indicated that requests had stayed the same, while 22 percent indicated that they had received no requests. Only 18 percent reported an increase while 15 percent reported a decrease. A look at the breakdown by admissions gives no clear indication of any trend by size.

Change in Requests for Amendments	>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	Total
Increased	40.7%	33.0%	22.8%	15.8%	14.0%	12.7%	18.4%
Stayed the same	25.4%	26.6%	36.6%	36.7%	36.8%	30.9%	33.5%
Decreased	0.0%	8.3%	20.0%	20.0%	20.4%	9.6%	15.0%
No requests	6.8%	14.7%	7.6%	19.2%	20.8%	36.3%	21.8%
Do not know	27.1%	17.4%	13.1%	8.3%	8.0%	10.5%	11.4%

The survey also asked respondents to indicate the **percentage of patients who requested information for amendments or corrections**. Of all respondents 87 percent reported that 2 percent or fewer patients requested amendments, with 33 percent showing no requests for such information.

Requesting Amendment or Correction	>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	Total
None	10.2%	17.4%	26.2%	31.3%	34.0%	47.1%	33.2%
0.1-2%	52.5%	59.6%	60.7%	56.3%	57.2%	43.9%	53.7%
2.1-4%	3.4%	3.7%	2.8%	2.1%	2.0%	2.2%	2.4%
4.1-6%	1.7%	0.9%	0.7%	0.4%	0.0%	0.3%	0.4%
6.1-8%	0.0%	0.0%	0.0%	0.8%	0.0%	0.0%	0.2%
8.1-10%	0.0%	0.0%	0.7%	0.0%	0.4%	0.0%	0.2%
Greater than 10%	0.0%	0.0%	0.0%	1.7%	1.2%	0.6%	0.8%
Do not know	32.2%	18.3%	9.0%	7.5%	5.2%	5.7%	9.0%

The HIPAA regulations let individuals know that they have the right to request a copy of their health information from covered entities. The 2006 survey asked: "Of the patients treated in your facility in the last year, what percentage of patients requested **copies of their health information?**" Eighteen percent reported that they had received no requests from patients in the last year. Twenty-three percent reported less than 5 percent had

requested copies, and 15 percent reported from 5 to 10 percent of their patients requested copies. At the other end of the spectrum, 11 percent of all respondents indicated that 25 percent or more patients requested copies.

Percent of Patients Requesting Copies	Percent of Facilities that Received Requests
None	18.3%
0.1-5%	23.3%
5.1-10%	14.7%
10.1-15%	10.7%
15.1-20%	5.1%
20.1-25%	6.5%
Greater than 25%	10.6%
Do not know	10.9%

Sixty-three percent of total respondents say they charge patients for copies of health information. Of these, 43 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. As noted in previous years, 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. Fifty-three percent report that their fee is governed by state regulation; 29 percent indicate there is a separate fee for non-patient representatives. This process is likely to change as electronic health records and personal health records evolve.

Security: The Next Challenge

The HIPAA security rule was in place for almost one year when the 2006 survey was taken. As in 2005, the survey asked if the facility had **designated a security officer**. This year, 100 percent of respondents indicated that their organization has a security officer, compared to 89 percent in 2005.

Why do so many more facilities have security officers than privacy officers? It may be that many organizations consider security an information technology function, so the role may have already existed in some form before HIPAA. Respondents were next asked to designate whether the security officer is full or part time. About two-thirds (65 percent) of respondents say the security officer role is a full-time one, compared to 57 percent in 2005.

Security Officer Status	Percent
Full-time	64.6%
Part-time	35.4%

A look at responses by facility size indicates larger facilities are slightly more likely to have a full-time position.

Security Officer Status	>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	66.1%	66.1%	71.0%	70.4%	68.8%	53.2%
Part-time	33.9%	33.9%	29.0%	29.6%	31.2%	46.8%

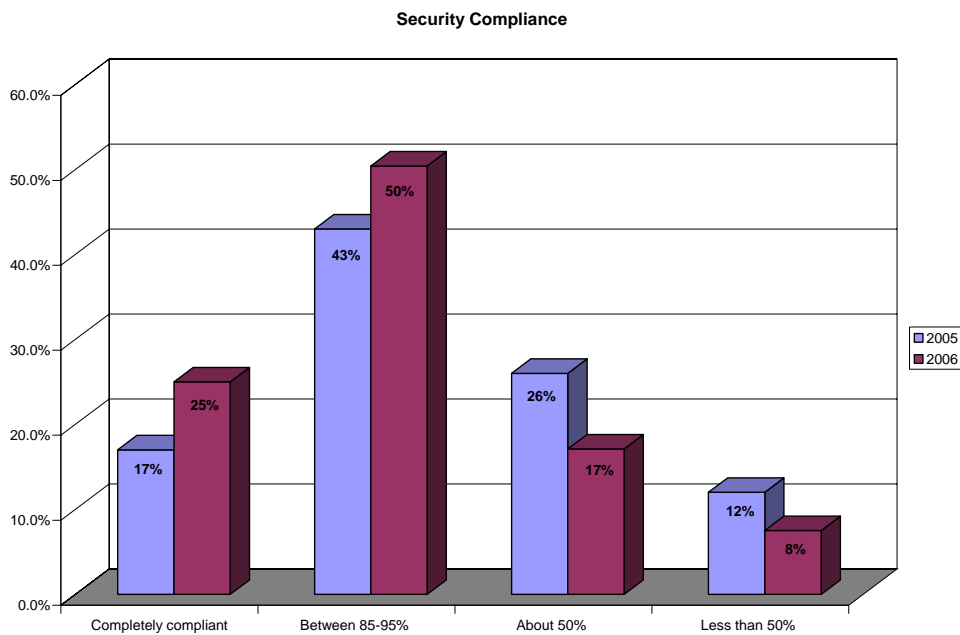
For those reporting a part-time director, 57 percent again indicated that the role was filled by an IT or information services employee. Only 4 percent reported that the privacy officer was also serving as the security officer. Ten percent of respondents indicated that an HIM professional held the part-time security officer role. The relatively high number of “other” responses continues to reflect small institutions’ need to share the load among administrators and individuals with skills in organization, auditing, and so forth.

Part-time Security Officers	Percentage
HIM/Medical record director	10.1%
Compliance officer	7.1%
Risk manager	3.0%
Privacy officer	3.8%
CIO	7.3%
IS or IT personnel	57.0%
Other	11.6%

The number of facilities that have a **committee or task force related to security** has decreased since 2005. In 2005 the figure for committees stood at 78 percent, but in 2006 the figure is 59 percent. The reasons why are not clear, but it may be that some of these duties have been assigned to a privacy committee or to the information technology department if the organization has completed its initial security review and adopted a security plan.

Security Task Force or Committee	2004	2005	2006
Yes	85.7%	78.7%	59.4%
No	14.3%	21.3%	40.6%

The number of respondents who believe their facilities are **compliant with HIPAA security** has increased. In 2006, 25 percent of respondents described themselves as completely compliant, and 50 percent described themselves as 85 to 95 percent compliant. This represents an increase over 2005, when 17 percent of all respondents described themselves as completely compliant, and 43 percent described themselves as 85 to 95 percent compliant. Clearly there is a high level of confidence in the industry that the security requirements have been met. This corresponds with the popular belief that the HIPAA security rule’s formula for compliance was easier to meet than that of the privacy rule, which has more external factors.



The results are also roughly consistent with facility size. More research is warranted to better understand trends among facilities by size.

Level of 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	Total
Completely	33.9%	31.2%	32.4%	21.3%	23.2%	22.0%	25.0%
Between 85-95%	50.8%	52.3%	43.4%	53.3%	48.4%	52.2%	50.4%
About half	10.2%	11.9%	13.1%	18.3%	20.0%	18.8%	17.1%
Less than 50%	5.1%	4.6%	11.0%	7.1%	8.4%	7.0%	7.5%

The survey asked if people had recently upgraded their electronic software/application systems to comply with HIPAA security requirements. The results find that 54 percent have upgraded recently, while 46 percent have not. We have noted below the type of software involved for those that did upgrade. Interestingly, the largest and smallest facilities were more likely to have upgraded.

Security Software/Applications Upgraded?	>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	Total
Yes	79.7%	71.6%	45.5%	41.3%	48.0%	62.7%	54.3%
No	20.3%	28.4%	54.5%	58.8%	52.0%	37.3%	45.7%

Firewalls, anti-virus software, and data back-up technologies were the most frequently updated.

What was Upgraded?	Percent
Firewall	40.4%
VPNs	25.9%
SSL technology	12.8%
Anti-virus/spyware/spam	38.2%
Remote access: restricted access	25.3%
Remote access: caller ID	14.4%
Remote access: callback	13.7%
Remote ID and authentication	19.9%
Data back-up technologies	30.2%
RAID technology	13.3%
Cryptographic technologies	13.3%
Single sign-on	15.0%
Biometric technology	6.6%
Access control technology	14.1%
Intrusion detection monitor/response	10.6%

Privacy, Security, and RHIOs

In light of the growth of health information exchange projects, health information networks, or regional health information organizations (RHIOs), the survey asked for the first time if **respondents were involved in these efforts from a privacy and security standpoint**. Thirty-one percent of respondents indicated they were involved in such a project. At this early stage, this statistic is not surprising; however, as individual organizations become more involved in RHIOs, we fully expect this number to increase.

Most of those respondents who are involved in RHIOs indicated that their **role is related to privacy and/or security**. Future research will attempt to get a better picture of RHIO involvement.

RHIO Roles	Percent
Privacy	34.1%
Privacy and security	28.0%
Security	32.4%
Other	5.5%

Privacy and Security Training: A Key Factor

Training and education have been important concerns for privacy officers and once again AHIMA asked respondents how they are training organization employees and volunteers.

The survey asked how facilities are handling **privacy training for new employees**. Sixty-four percent indicated that new employees are trained in-house by either the privacy officer or an education officer. It is clear from responses, however, that many facilities are using multiple forms of education depending on the situation and the size of the facility.

	>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	Total
New Employee Privacy Training							
In-house by privacy/education officer	64.4%	69.7%	77.2%	80.7%	79.1%	79.3%	64.4%
In-house by external trainer	3.4%	5.5%	4.1%	5.5%	5.2%	4.5%	3.4%
In-house by facility counsel	1.7%	7.3%	6.2%	8.4%	4.0%	4.5%	1.7%
Instruction external to facility	5.1%	7.3%	14.5%	14.7%	14.9%	6.7%	5.1%
Video instruction developed by facility	23.7%	26.6%	16.6%	13.4%	12.4%	15.3%	23.7%
Video instruction from external source	13.6%	7.3%	11.7%	13.0%	17.7%	21.7%	13.6%
Web-based instruction developed internally	37.3%	44.0%	20.0%	18.9%	17.7%	14.6%	37.3%
Web-based from external source	16.9%	7.3%	15.9%	10.9%	8.4%	8.0%	16.9%

For **ongoing training for current employees**, training methods varied considerably. Department staff meetings, newsletter articles, and reminders topped the list.

	>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	Total
Methods for Annual Privacy Training							
Posters	8.3%	13.7%	24.8%	32.2%	38.1%	41.9%	8.3%
Table tent signs	22.9%	24.2%	19.8%	15.6%	9.8%	5.6%	22.9%
Contests	6.3%	12.6%	6.6%	8.8%	6.5%	7.0%	6.3%
Newsletter articles	64.6%	57.9%	42.1%	32.7%	32.1%	33.7%	64.6%
Reminders	56.3%	50.5%	30.6%	25.4%	34.4%	41.1%	56.3%
Additions to job description	20.8%	20.0%	19.8%	16.1%	14.9%	18.5%	20.8%
Programs/skits	0.0%	10.5%	6.6%	8.3%	10.7%	12.2%	0.0%
Announcements	33.3%	22.1%	14.0%	13.2%	11.6%	16.7%	33.3%
Department staff meetings	68.8%	57.9%	38.0%	37.1%	31.2%	49.3%	68.8%

Information on the Go: Outsourcing

Outsourcing continues to be an HIM issue in some areas of the country. Of those responding, 43 percent indicated that their organization is **outsourcing in the area of health information management functions**.

(The response is very similar to the 42 percent reported in 2005.) The practice of outsourcing appears to have a direct relationship to the size of the organization.

	>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	Total
Outsource							
Yes	64.4%	58.7%	51.7%	48.8%	41.6%	27.1%	43.2%
No	35.6%	41.3%	48.3%	51.3%	58.4%	72.9%	56.8%

According to responses from those who outsource, transcription is **most frequently outsourced**, followed by release of information and coding. The survey did not ask if the functions were outsourced to companies out of state, out of the country, or just out of the facility. Again, results vary with facility size.

	>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	Total
Areas Outsourced							
Transcription	78.4%	65.1%	52.2%	50.5%	55.9%	58.0%	78.4%
Coding	16.2%	33.3%	39.1%	39.4%	28.0%	24.7%	16.2%
ROI/Disclosure	75.7%	58.7%	49.3%	43.1%	38.7%	37.0%	75.7%

Outsourcing of protected health information requires a business associate contract, according to HIPAA. However, some outsourcing vendors in turn outsource their business, so it is possible that work might be given to firms overseas. This has been a concern to some state legislators, so the survey asked whether facilities' **business associate contracts address the use of subcontractors to offshore affiliates or companies**. Forty-nine percent responded yes, while 30 percent indicated that their business associate agreements did not address this issue and 21 percent were not sure. In text responses, several respondents commented that they would be reexamining their agreements as a result of considering this question.

	>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	Total
Business Associate Contract Addresses Outsourcing							
Yes	51.9%	56.9%	46.3%	49.7%	47.5%	47.6%	48.9%
No	25.9%	19.6%	36.3%	27.5%	35.6%	31.0%	30.1%
Not Sure	22.2%	23.5%	17.5%	22.8%	16.9%	21.4%	21.0%

Conclusion

Three years after the implementation of the HIPAA privacy rule, the AHIMA survey concluded the following conclusions:

- **The majority of facilities continue to be essentially compliant with HIPAA privacy and security regulations.** Unfortunately, the number of those who believe that they are 85 percent or more compliant with privacy has dropped in the last year. Responses to other questions give insight into this slight decrease and show that while it is not a significant change, it is enough to raise concern.
- **Barriers to full compliance such as a lack of resources and diminished administrative support should be addressed.** For the second year in a row, respondents indicate they need more staff, time, ongoing education programs, and support from organization and medical staff leaders. Responses to questions and comments indicate that there is not enough time available to do the education that privacy officers feel is needed, and as a consequence they are noticing that some old habits are creeping back. This concern does not appear to be reflected in patient complaints, but it is clear that staff at all levels need to be continually reminded of the need to maintain privacy. The issue of budget also appears to impact the level of privacy training and monitoring that a privacy officer or staff are capable of providing. Finally,

privacy officers report sensing a loss of support from senior management, both in ensuring the facility staff is aware of the need for privacy as well as ensuring sufficient budgeting for education.

- After three years, most providers are growing accustomed to the various provisions of the privacy rule, but there are still reports of **difficulties with a select few requirements**.
- Not surprisingly, **many respondents would like to see changes in the accounting for disclosures provision** of the privacy rule. Most commonly, respondents had received only a few requests for an accounting or none at all. For many, this provision is not only burdensome but also significantly inefficient. This problem could be easily addressed while ensuring that individuals would have an accounting for all releases not covered by authorization or law.
- **It appears that the security regulations were much easier to achieve than the privacy rule.** One year into the HIPAA security regulations, a quarter of the surveyed facilities reporting indicate compliance at the top level with another 50 percent indicating that they are close to full compliance.
- Some **consumers are becoming more aware of the importance of the privacy of health information**, as evidenced by the increased number of questions providers report being asked by patients. More disturbingly, nearly a quarter reported encountering consumers who refused to sign release of information forms. More research is needed to understand how deep those fears are or what consumers are most worried about. Clearly the industry now has an opportunity to educate consumers on how their personal health information will (or should) be protected. This is an important step. Without consumer confidence the national health information network will never succeed.

HIPAA implementation has been a challenge for organizations, and it appears that for the majority the challenge has been met. However, the need for privacy, confidentiality, and security remain, especially as organizations tighten staffing and budgets. A slight drop in the number of facilities reporting themselves to be fully or mostly compliant with HIPAA should serve as a warning to the industry that compliance should not be taken for granted.

If the support for privacy and security and the need for ongoing training are not maintained (and, in a few areas, increased), all the work that has been put into the HIPAA compliance efforts of the last few years may be undone over time.

The need for support of privacy and security must also reach beyond facilities. The federal government's approach to HIPAA enforcement has been to educate rather than fine or prosecute offenders. While we applaud this approach, a concerted effort to educate and remind the healthcare industry and others of the need to maintain and continually improve privacy efforts is equally needed.

The healthcare industry has much to learn from the lessons of HIPAA as it moves toward electronic health records and a nationwide health information network. There is considerable disagreement on whether electronic health records will improve privacy or security and there are many concerns on how information networks will protect data. Consumers will be watching the healthcare industry to see how well it complies with the HIPAA rules before they put their trust in a national health information exchange. Communicating with consumers, answering their questions and addressing their concerns, may be a key to advancing health information exchange activities. Privacy officers and HIM professionals will be important partners in this process. AHIMA believes that the time is right for an open dialogue about the value of privacy and security at both the national and organizational levels.