The State of HIPAA Privacy and Security Compliance

A report by the
American Health Information Management Association
April 2004

AHIMA is the national association of health information management professionals (HIM) whose more than 46,000 members are dedicated to the effective management of the personal health information needed to delivery 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 additional information about AHIMA, visit www.ahima.org.

Contributors:
Donald Asmonga, MBA
Jill Burrington-Brown, MS, RHIA
Jill Callahan Dennis, JD, RHIA
Sue Fiorio
Kevin Gould
Scott MacKenzie
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

Contents

Executive Summary 4

Historical Perspective 8

Survey Results and Analysis.....12

Conclusion 38

Executive Summary

"Despite all the anxiety over this issue, it appears as if healthcare organizations are integrating HIPAA privacy into their culture and are seeing positive results."

Linda L. Kloss, MA, RHIA
Executive Vice President, Chief Executive Officer
American Health Information Management Association

Overview

April 14, 2004, will mark the first anniversary of the implementation of the Health Insurance Portability and Accountability Act (HIPAA) final privacy rule. This long-awaited regulation represented a critical step in the development of national standards for the use and disclosure of personal health information. Many in the healthcare industry, including the American Health Information Management Association (AHIMA), supported its development and recognized its importance in protecting the privacy, confidentiality, and security of health information.

But even before it took effect, the HIPAA privacy rule created concern within the healthcare industry regarding implementation and compliance. So where does the industry stand with HIPAA now—one year after implementation?

To find out, AHIMA conducted a survey to assess the current state of HIPAA privacy within the healthcare industry. AHIMA asked the people closest to this issue—the individuals working on the planning, training, and ongoing compliance of HIPAA privacy regulations primarily in hospitals and health systems—to give us their feedback.

AHIMA releases the results of this research in conjunction with the first annual National Health Information Privacy and Security Week, April 11-17, 2004. 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.

Profile of Respondents

The 1,192 survey respondents consisted of 58 percent designated privacy or security officials, 11 percent who are functioning as privacy or security officials without the formal titles, and 31 percent who have served on the HIPAA privacy and security teams or committees.

A little more than two thirds of the respondents work in the hospital or healthcare system setting.

Majority of Organizations Achieving Significant Compliance

Nearly a year after the final privacy rule took effect, 68 percent of respondents feel their facilities are currently between 85 to 99 percent compliant while only 8 percent report being 50 percent or less compliant at this time. Twenty-three percent (23 percent) of the respondents feel that their organization is fully compliant.

Problem Areas Uncovered

One clear outcome of the implementation of the HIPAA privacy requirements was the identification of deficiencies with existing business practices or procedures that put privacy of patient information at risk. Seventy percent (70 percent) of survey respondents agree that HIPAA uncovered privacy problem areas within their facilities. The two most common responses related to the lack of standardized practices for release of information and public access to personal health information.

The HIPAA rule requires facilities to handle complaints regarding their privacy practices. A little more than half of the respondents indicated that their facilities have received complaints from individuals (patients) regarding the HIPAA rule or their rights. It should be noted that some complaints could simply be misunderstandings of the new requirements rather than actual HIPAA violations.

One additional area identified by write-in responses as a source of difficulty is the interaction of the HIPAA privacy rule with the Family Educational Rights and Privacy Act (FERPA). Respondents from college and university health settings indicated a struggle to determine whether or not their records fall under HIPAA or FERPA. This bears further review and clarification by federal policymakers.

Compliance Challenges

When asked about current problems complying with the privacy requirements, no single area was identified by more than 39 percent of respondents. However, four areas emerged as more problematic than all others:

- Accounting for release of protected health information (39 percent)
- Obtaining protected health information from other providers (33 percent)
- Access and release of information to relatives or significant others (32 percent)
- Business associate requirements (25 percent)

Need for Modification

The areas indicated as most problematic within the privacy rule are the same areas respondents feel need to be modified by the federal government. The clear leader in this group with more than half of respondents is accounting for release of protected health information (51 percent). This problem has consistently been identified in other, more informal, surveys and in testimony given to the National Committee on Vital and Health Statistics (NCVHS).

Other areas respondents would like to see addressed include business associate requirements (20 percent) and access and release of information to relatives or significant others (18 percent). Twenty-five (25 percent) of survey respondents prefer no further modifications be made at this time.

HIPAA and State Laws

HIPAA allows for state preemption, which means that more restrictive state laws may supersede HIPAA privacy requirements. While many healthcare organizations were worried about the confusion this might cause, the majority of respondents (77 percent) indicated that no problems had yet been experienced.

Unless required by the state, HIPAA provides facilities the option as to whether or not to obtain patient consent for disclosures of protected health information for **treatment, payment, and healthcare operations** (TPO). The survey results shows that some facilities have decided to request patient consent for the disclosure of protected health information for TPO even though it may not be required by state law. Fifty-one percent (51 percent) of respondents indicated their facilities request patient consent for the disclosure of protected health information for TPO consent while only 34 percent indicated their state requires it.

Reaction to HIPAA

When asked about the reaction of **staff** to changes in organizational policies and procedures related to HIPAA, 81 percent of respondents indicated that staff was either very supportive or somewhat supportive.

When asked about the reaction of **patients** to changes in organizational policies and procedure related to HIPAA, respondents felt that patients were more supportive now than they were a year ago. Respondents indicated that 51 percent of patients were currently either very supportive or somewhat supportive versus 39 percent a year ago.

Organizational Resources Dedicated to HIPAA

Staff Resources

The survey reveals that while 85 percent of the respondents report the existence of a committee or task force related to privacy and security, fewer than half (45 percent) of the respondents indicated their facilities employ a full-time privacy official. In those organizations where a full-time privacy official is not in place, the responsibilities of this position fall to the director or manager of HIM in 63 percent of the cases. AHIMA plans to investigate the factors that determine whether or not an organization employs a full-time privacy official.

The majority of reported respondents indicated that their facilities have both a security task force (82 percent) and a designated security officer (80 percent), with 57 percent indicating that the security officer role is handled by IS or IT personnel.

Software and Systems Resources
More than half of the respondents said that HIPAA privacy implementation required some kind of upgrade to electronic software or application systems. Nearly three quarters of those facilities performed the upgrade internally or used an existing vendor.

Only 44 percent of respondents said the purchase or development of new software was required as part of HIPAA privacy and compliance. In facilities where new software was implemented, the main reasons were accounting for disclosures (55 percent), privacy notice acknowledgement tracking (32 percent), admissions/registration (31 percent), and patient accounting/billing/collections/claims (31 percent).

Interestingly, only 8 percent of respondents indicated their current identifiable budget for HIPAA privacy compliance exceeded $100,000, while 34 percent indicated that there was no budget at all. This reinforces that successful privacy and security compliance is more about sound policies and procedures than technology.

Summary

As we approach the one-year anniversary of the implementation of the HIPAA final privacy rule, the message from the industry regarding HIPAA privacy and security compliance is a positive one.

The majority of facilities are significantly compliant. While most are still striving to achieve total compliance, part of the reason may be a few problem areas identified within the compliance requirements. The industry has indicated that these areas need to be addressed for modification. The Department of Health and Human Services (HHS) is currently considering modifications to the privacy rule.

The privacy rule has helped a majority of organizations identify where policies and procedures need to be improved to ensure the privacy of protected health information. The majority of staff and patients are supportive of new privacy policies and procedures.

Implementation and compliance have been achieved primarily through the use of existing staff and resources, illustrating that HIPAA has not been the overwhelming burden to the healthcare industry that was predicted by opponents of the privacy rule.

AHIMA intends to conduct this survey annually to provide the industry with important information regarding the status of HIPAA privacy and security compliance.

The HIPAA Privacy Rule: A Historical Perspective

"In this regulation, we must balance individuals' privacy interests against the legitimate public interests in certain uses of health information."

Department of Health and Human Services
(Federal Register, vol. 65, no. 250, p. 82566, December 28, 2000)

On April 14, 2003, the Health Insurance Portability and Accountability Act's covered entities[1] were required to be in compliance with the final HIPAA standards for privacy of individually identifiable health information. Small health plans (plans with annual receipts of $5 million or less) were provided an exception to this requirement. Small health plans were provided an additional year—until April 14, 2004—to become compliant with the final privacy rule.

The HIPAA final privacy rule was one of several components required under the administrative simplification[2] provisions of the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191). Previously known as the Kennedy/Kassebaum[3] bill, this legislation was signed into law on August 21, 1996, with the formal intention of improving the "portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud and abuse in health insurance and healthcare delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes."

The purpose of the administrative simplification provisions were to "improve the Medicare program under title XVIII of the Social Security Act, the Medicaid program under title XIX of the SSA, and the efficiency and effectiveness of the health care system, by encouraging the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information." The legislative language provided the secretary of Health and Human Services the authority to adopt standards for:

- Transactions[4]
- Unique health identifiers for individuals, employers, health plans, and healthcare providers

[1] Covered entities are defined by the HIPAA law as health plans, healthcare clearinghouses and healthcare providers who conduct certain and financial and administrative transactions electronically (PL 104-191).
[2] PL 104-191, Title II—Preventing Health Care Fraud and Abuse; Administrative Simplification; Medical Liability Reform—Subtitle F, Administrative Simplification.
[3] Senator Edward M. Kennedy (D-MA) and Senator Nancy Landon Kassebaum (R-KS).
[4] Transactions pertain to financial and administrative transactions including 1) Health claims or equivalent encounter information; 2) Health claims attachments; 3) Enrollment and disenrollment in a health plan; 4) Eligibility for a health plan; 5) Health care payment and remittance advice; 6) Health plan premium payments; 7) First report of injury; 8) Health claims status; and 9) Referral certification and authorization.

- Code sets[5]
- Security standards for health information
- Electronic signature
- Transfer of information among health plans

For additional information on the specifics of the standards and the adoption timetables, visit the Department of Health and Human Services' administrative simplification Web site at http://aspe.hhs.gov/admnsimp/index.shtml.

At the time of HIPAA's enactment, Congress was well into several years of discussion on health information privacy legislation that would establish national standards for the use and disclosure of personal health information. Progress on legislation was difficult, as a range of issues seemed to regularly confound the debate. Some of the issues causing friction included:

- Whether or not privacy legislation would completely preempt state law allowing for the establishment of a federal "ceiling" of protections
- The situations under which consent or authorization would be required
- What entities would be covered by legislation
- The level of penalties for infractions
- Unique healthcare identifiers
- Access to information for health research
- Marketing

Understanding the complexities involved with passing privacy legislation but knowing something would have to be done prior to the adoption and use of electronic financial and administrative transactions, Congress gave itself an ultimatum in the HIPAA administrative simplification provisions. Along with establishing federal penalties for the wrongful disclosure of individually identifiable health information in the language, Congress gave itself 36 months from the date of HIPAA enactment (August 21, 1996) to pass health information privacy legislation. Therefore, if Congress did not pass health information privacy legislation by August 21, 1999, the secretary of Health and Human Services would be required to promulgate final regulations containing health information privacy standards by February 21, 2000. The regulations were required, at minimum, to address:

- The rights that an individual who is a subject of individually identifiable health information should have
- The procedures that should be established for the exercise of such rights
- The uses and disclosures of such information that should be authorized or required

[5] A code set is defined as "any set of codes used for encoding data elements, such as tables of terms, medical concepts, medical diagnostic codes, or medical procedure codes."

In addition to the final regulations, the secretary of HHS was required to provide privacy recommendations to Congress pertaining to the above topics within one year of the enactment of HIPAA—August 21, 1997. Further, the HIPAA legislation required that the final regulation be preemptive only to the point where it would preempt less stringent state laws. Any state law that was deemed stronger that the HIPAA final privacy regulation would remain in effect and states would be permitted to pass laws that were stronger than HIPAA. The preemption concern exists to this day and is addressed in the survey. Finally, the administrative simplifications in HIPAA required the secretary of HHS to consult with the National Committee on Vital and Health Statistics (NCVHS),[6] whose responsibilities were statutorily changed by this legislation.

A HIPAA Privacy Timeline

Date	Privacy Event
8/21/1996	Enactment of the Health Insurance Portability and Accountability Act
9/11/1997	HIPAA required recommendations of the secretary of HHS on the confidentiality of individually identifiable health information provided to Congress
8/21/1999	Congress' self-imposed deadline to pass privacy legislation
11/3/1999	Secretary of HHS promulgation of the notice of proposed rulemaking (NPRM) for standards for privacy of individually identifiable health information
2/17/2000	End of public comment period on the NPRM
12/28/2000	Publication of final rule for standards for privacy of individually identifiable health information
1/21/2001	Deadline to publish final rule for standards for privacy of individually identifiable health information
2/28/2001	Bush administration opening of public comment period on final rule due to Clinton administration administrative error where Congress was not notified of the publication of a major rule
3/30/2001	Closing of second comment period on the final rule
4/14/2001	Effective date of the final privacy rule. Covered entities required compliance within two years. Small health plans required compliance within three years
7/6/2001	HHS publication of guidance document for compliance with the final rule
3/27/2002	HHS publication of NPRM for modifications to the final rule for standards for privacy of individually identifiable health information
4/26/2002	Closing of comment period on NPRM for modifications for the final rule
8/9/2002	HHS publication of final modifications
10/8/2002	HHS publication of complete final rule for standards for privacy of individually identifiable health information

[6] For further information on NCVHS, visit http://www.ncvhs.hhs.gov/.

12/4/2002	HHS Office of Civil Rights publication of guidance document for compliance with the final rule
3/13/2003	HHS Office of Civil Rights publication of frequently asked questions pertaining to the final rule
4/14/2003	Final date for covered entities to reach compliance with the final rule
4/17/2003	HHS publication of an interim rule for enforcement and penalties
4/14/2004	Final date for small health plans' compliance with final rule

In developing the final privacy rule, the Department of Health and Human Services received more than 52,000 public comments. Both the NCVHS and congressional groups, including the House Ways and Means Committee, the House Energy and Commerce Committee, and the Senate Health, Education, Labor and Pensions Committee, held numerous hearings before and after the publication of the final rule.

Through public comments, hearing testimony, and articles on the privacy rule, a great deal of information was offered as to why establishing privacy standards was critical, and positive suggestions were provided as to how to improve the privacy rule. Unfortunately, some individuals and industry organizations also offered misstatements, false assumptions, and grim predictions to describe their perceived impact of the rule.

Summarizations of a few of these statements are offered below:

- The privacy rule would require facilities to erect soundproof walls and provide all patients with private rooms
- The minimum necessary provision would not permit doctors and other caregivers the ability to share health information in conversation or for treatment
- Family members and friends would be prohibited from picking up prescriptions for their siblings or parents
- It would be a flawed and unworkable regulation that is unnecessarily complex. It would be impossible to achieve compliance
- The notice of privacy practices would be voluminous (10 to 20+ pages) and intimidate patients
- The rule would be a detriment to the cost-effective delivery of care
- It would be nearly impossible to achieve compliance
- The cost of compliance would be substantially higher than the $17 billion over 10 years projected by the Department of HHS (one estimate indicated $43 billion over five years)
- Preemption would be an unworkable burden that will cause confusion

These misinterpretations and misstatements, combined with the sentiments against the rule's provisions, were used as a reason for a call to delay the April 14, 2001, implementation date of the final privacy rule—knowing that compliance was not required until April 14, 2003. Ultimately, the secretary of Health and Human Services did not delay the effective date of the privacy rule, ensuring a compliance date of April 14, 2003.

Survey Results and Analysis

"A lot of time and energy was spent prior to the arrival of HIPAA. It reinforced the importance of confidentiality to all staff—something that health information management staff work with every day."

Survey respondent

Why AHIMA Conducted This Survey

From the time that the Clinton administration presented the "final" HIPAA[7] privacy rule (often referred to in this paper and elsewhere as the privacy rule, the rule, or HIPAA privacy regulations) on December 28, 2000,[8] concerns were raised about a variety of aspects of the rule and its impact on patients and the healthcare industry. It was predicted that various covered entities would spend vast sums to implement and remain compliant with the rule.[9] It was also predicted that mass confusion and hysteria would ensue when the rule was put in place.

In the fall of 2003, the NCVHS Subcommittee on Privacy and Confidentiality[10] held the first of several hearings to ascertain the status of the privacy rule, which had been implemented[11] on April 14, 2003. At the time, AHIMA informally surveyed its members to gain some insight into the state of the rule, because it had fallen to many of them to implement and ensure compliance with the rule in their organization.

While the informal AHIMA survey helped the Association put together testimony for the November 2003 hearing, it was clear that a more in-depth survey would be helpful. AHIMA decided to undertake such a survey and publish the results at the anniversary of the rule's compliance date and the Association's celebration of a National Health Information Privacy and Security Week, April 11-17, 2004.

The 2004 Survey Process

In February 2004 AHIMA, with the assistance of an impartial third-party market research firm, conducted a Web-based survey on the state of HIPAA privacy and security compliance. An e-mail invitation was sent to AHIMA members who were considered

---

[7] Health Insurance Portability and Accountability Act of 1996 (P.L. 104-191). See "Historical Perspective" section.

[8] *Federal Register,* vol. 65, no. 250, December 28, 2000.

[9] Covered entities are defined by the HIPAA rule §160.103 as "health plan(s)," " health care clearinghouse(s)," or "a health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter."

[10] The NCVHS was given a role as HIPAA advisor to the secretary of Health and Human Services for all aspects of the HIPAA law by the 1996 act.

[11] The HIPAA privacy rule was effective April 14, 2001, and called for a two-year implementation period for all covered entities except defined "small health plans." Thus April 14, 2003, became the HIPAA privacy rule compliance date for most of the covered entities.

most likely to have participated significantly in the HIPAA implementation process and to non-members who had participated in various HIPAA-related educational opportunities provided by AHIMA.

The survey instrument itself began with a question used to screen out those respondents who were not considered the most qualified to participate in this study. The combined result of an initial targeted invitation, one reminder e-mail, and the screening process resulted in 1,192 qualified responses to this survey. In keeping with the makeup of the AHIMA membership and qualified non-members, 56 percent of responses came from those working in the hospital setting. 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, Washington, DC, and Puerto Rico.

The members and non-members affiliated with AHIMA represent 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, these members have taken on this charge in a number of different healthcare settings. In many cases, they have been charged with the HIPAA privacy mandate. Where possible, we have included illustrative anonymous quotes that represent a sample of the remarks made by members in the survey.

With this survey (and future surveys), 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 information to provide maximum benefits to its patients.

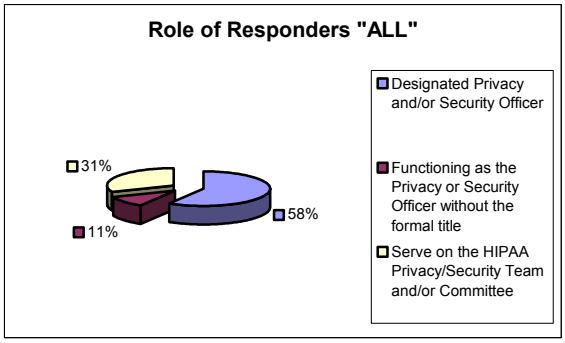
RESPONDENTS

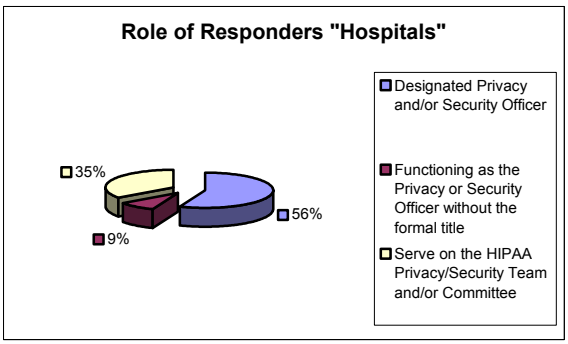
*"We gained better control over release of information. We became more efficient in dealing with visitors that were slowing down patient care. We now have a controlled environment for visitors that has allowed our physicians to see more patients in a more timely fashion."-- **Survey respondent***

The survey received responses from 1,192 individuals who work on planning, training, and ongoing compliance with the HIPAA privacy regulations in their organizations. The survey provided AHIMA with some insights on the state of HIPAA compliance.

The survey asked about the **role of respondents in regard to HIPAA implementation**. The survey respondents were made up of 58 percent designated privacy or security officers, another 11 percent who function as privacy or security officers without the formal titles, and 31 percent who have served on the HIPAA privacy and security teams or committees. The survey revealed that while 86 percent of the respondents reported the existence of a committee or task force related to privacy and security, fewer than half (45

percent) of the organizations represented employ a full-time privacy official. In organizations where a full-time privacy official was not in place, the responsibilities of this position fell to the director or manager of health information management (HIM) in 63 percent of the cases.

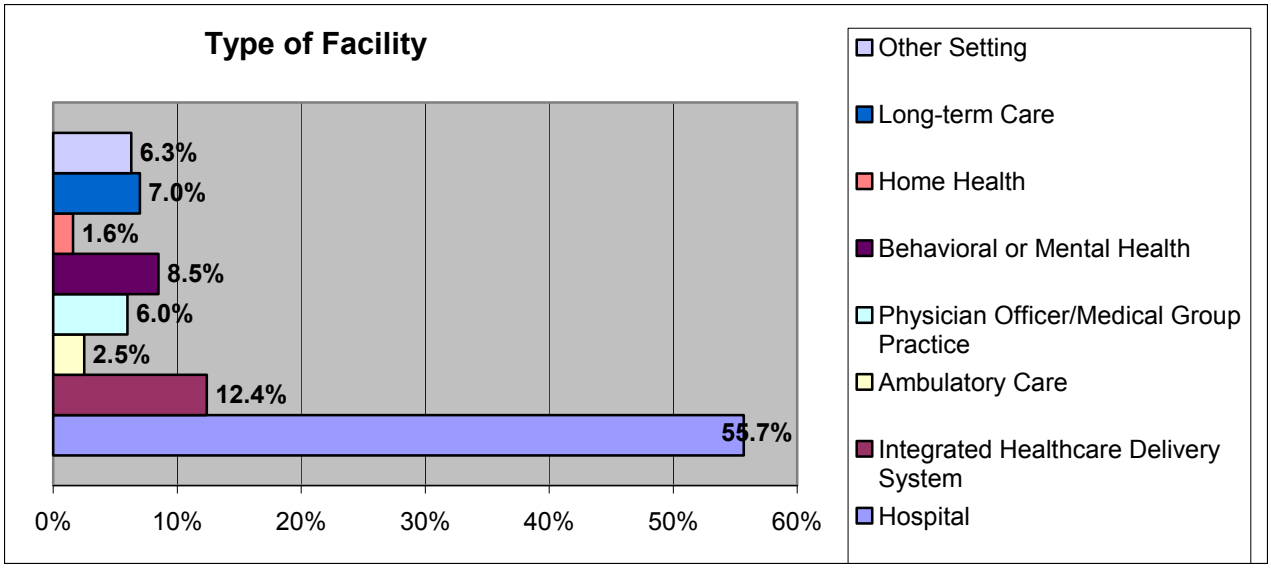




AHIMA was not surprised to see that approximately 30 percent of respondents were not privacy or security officers. For a variety of reasons, organizations chose privacy officials from among a number of potential candidates.

Types of Facilities

The types of facilities responding to the survey were also not surprising because at this time, other than hospitals, only larger facilities are more likely to employ certified health information managers, whereas many smaller organizations do not. The **facility breakdown** for the study included:



Staffed Inpatient Beds

To ascertain the size of responding facilities, AHIMA also asked hospital respondents to provide size by **staffed inpatient beds**. This would assist in analyzing how answers to other questions were affected by facility size. The bed size for the sample was:

Base:664	**Hospitals**
Over 500	7.8%
300-499	13.4%
150-299	25.5%
75-149	20.0%
Less than 75	33.3%

While this number was helpful, more details regarding the type of facility and size will be needed in the future to look at the state of healthcare privacy and confidentiality. Facilities have a considerable number of potential variations that may affect compliance, such as relationship to medical staff and organization.

PRIVACY ROLES

*"We had statewide meetings with all of the facility personnel that would be involved, along with our legal department and consulting group, to customize HIPAA policies that addressed our needs. This was very effective."--**Survey respondent***

The privacy rule requires that the covered entity designate a privacy official. The rule's detractors initially raised concerns that this would cause considerable expense and would become a burden. AHIMA had indicated early on in the debate that it fully expected that large organizations would hire a full-time privacy official similar to other industries, but that many would choose to handle the function on a part-time basis, generally placing the functions of the official in an existing position.

Full-time Privacy Official

The question of **whether the facility has a full-time privacy official** was answered as follows:

Full-time Privacy Officer	All	Hospitals
Yes	44.6%	39.2%
No	55.4%	60.8%

As expected, as hospital size decreases, so does the percentage of full-time privacy officials. Seventy-one percent of the hospitals of 500 beds or more reported a full-time privacy official, while only 25 percent in hospitals of 75 beds or less did. Although a privacy official must be designated by a covered entity, the functions that support or impact the privacy rule do not necessarily have to be fulfilled by the privacy official. For instance, in most hospitals release of information (ROI) functions are performed by the health information or medical record department, not a privacy official. Mid-size to large facilities that have a patient ombudsman or patient relations department might take an initial complaint on behalf of the privacy official.

A second question asked **who was the designated privacy official when there was no full-time privacy official**.

Designated Privacy Officer	All	Hospitals
HIM/Medical record dir/manager	62.7%	68.1%
Other	17.3%	13.1%
Compliance officer	12.1%	10.9%
Risk manager	3.5%	4.5%
IS or IT personnel (Director/Mgr)	2.4%	2.0%
CIO	1.5%	1.0%
Security officer	0.5%	0.5%

"All" was based on 660 responses and "Hospitals" on 404. Not surprisingly, almost 63 percent of the part-time privacy officials were HIM directors or managers. The second highest category of "compliance officers" came in at 12 percent. It is not clear if these were full-time or part-time compliance officers since many facilities, required by Medicare to appoint a compliance officer, have also met that rule with a part-time designation. AHIMA also found that in ambulatory care organizations, 91 percent of the positions filling the privacy offer role were HIM directors or managers. Long-term care organizations also had a significantly high level of HIM involvement at 74 percent.

While the "Other" category was initially a surprising percentage, a follow-up question identified a variety of areas, usually small facilities, groups, or practices, where existing officers took on the role of privacy officer. Again, this is not unusual for small entities. Administrators, CEOs, attorneys, CFOs, social service directors, nursing administrators, patient relations managers, quality managers, and others were identified. In all, nearly 100 different job titles were designated as serving in this capacity.

Committee or Task Force

AHIMA had recommended that covered entities appoint a committee or task force to oversee privacy and security implementation, including on-going activities associated with the HIPAA rule. We were pleased to see that 85 percent of the responding organizations and nearly 90 percent of hospitals have formed such committees. Again, we suspect the cases where no committee was formed occurred in the smallest of entities.

COMPLIANCE

*"HIPAA privacy increased everyone's awareness and provided uniform education about privacy."--**Survey respondent***

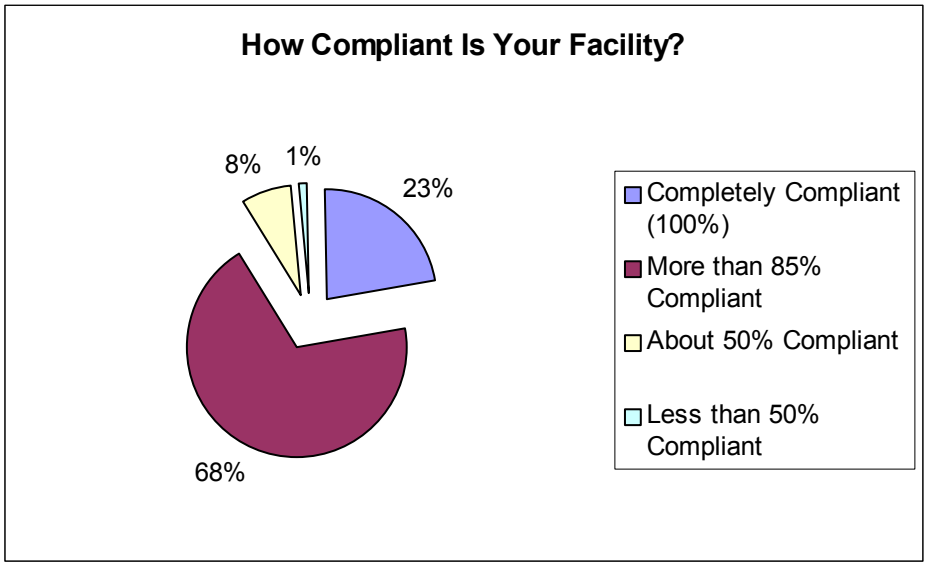
It is critical to remember that compliance is and will be an ongoing process. Judging the level of compliance in an organization is not an exact science. Compliance is subject to individual circumstance and interpretation. With the changing environment and regulations related to health information privacy, both before and after the April 14, 2003, compliance date, we believe it is almost impossible to be judged by all stakeholders as completely compliant. For instance, under specific situations the "business associate" requirements for the rule's covered entities were extended until 2004. Various state legislatures have also enacted health information privacy rules during the implementation and compliance periods, so covered entities have found themselves in shifting sands with the issue of privacy and confidentiality compliance.

The HIPAA privacy rule has been interpreted by a large number of equally authoritative experts who gave opinions that were varied and contradictory. To some extent, this created an environment in which many covered entities, patients, government authorities, and the press were thoroughly confused as to what constitutes compliance. This confusion has been pointed out in NCVHS testimony and in the press. AHIMA hopes that as the healthcare industry continues its quest for compliance, a more accurate reading and consensus on the correct interpretations will emerge.

Levels of Compliance

It is important to remember that in the HIPAA context, compliance is a continuous process, not a final destination. Despite the changing nature of compliance, AHIMA asked several questions about it. The first was: **"In your opinion, how compliant is your facility with the HIPAA privacy requirements?"**

The vast majority (68 percent of respondents) reported at least 85 percent compliance. Only 23 percent believed that their organization was 100 percent compliant with the HIPAA privacy requirements:

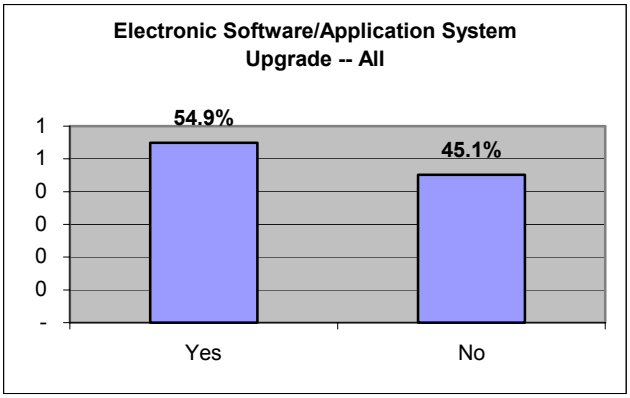


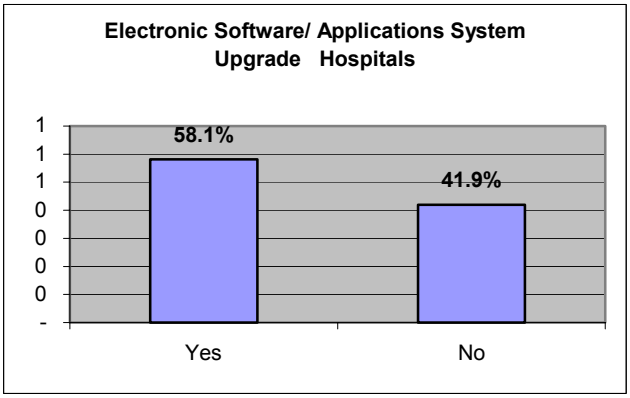
The 85 to 100 percent range leaves room for error, but it is comforting to know that in spite of predictions of chaos in the environment, some 91 percent of the respondents believed themselves close to full compliance.

While approximately 9 percent were at or below an estimated 50 percent compliance, it appears that the facilities most concerned about their level of privacy compliance were long-term care, behavioral health, and home health. It should be noted that each of these types of facilities has some unique challenges with privacy because care is delivered in group settings and in the home.

System Changes

Because many covered entities expressed concern about the amount of system changes that would be necessary to implement the HIPAA rule, AHIMA asked: "**Did your facility's HIPAA privacy implementation require an upgrade of your electronic software/application system?"** A full 55 percent of respondents said yes.





For those who responded that their facility's HIPAA privacy implementation required an upgrade, **we then asked how the upgrade was completed**:

Upgrade Completed:	All	Hospitals
Internally or with an existing vendor	73.1%	78.2%
Using a new vendor	5.5%	3.6%
Both	21.4%	18.1%

"All" was based on 654 responses and "Hospitals" was based on 386 responses. Often, systems changes will vary between vendor and user depending on the size of the organization and its IT staff component. Moreover, in the case of the privacy rule, the extent that an electronic means to compliance was chosen affected responses. We assume that systems changes could also vary by how "electronic" (fully computerized) a facility, group practice, or provider has become. Conceivably, a small provider could be compliant with HIPAA without electronic systems changes, depending on paper logs and notices within its patient record. A large, fully electronic facility would require considerable systems changes.

The introduction of software changes involving a new vendor was limited to just 27 percent of the time, which was likely a surprise to many who expected a number of new vendors on the scene.

We also asked if **new software was purchased or developed for HIPAA compliance:**

New Software Purchased or Developed	All	Hospitals
No	55.5%	55.6%
Yes, purchased	24.8%	25.8%
Yes, developed in-house	19.6%	18.7%

Only 44 percent of those surveyed report purchasing or developing new software as part of HIPAA. Of those who purchased or developed software, the largest number, 55.3 percent (61.7 percent in the "Hospital" category) report such software as addressing the "accounting for disclosure" function. Anecdotally, most AHIMA members continue to report that this is the one function that remains incomplete within their systems.

When asked **what functions purchased or developed software addressed,** respondents indicated**:**

Function	All	Hospitals
Accounting for disclosures (new or revision of MR/EHR functions)	55.3%	61.7%
Privacy notice acknowledgement tracking (new)	31.9%	32.5%
Admissions/registration	31.1%	31.9%
Patient accounting/billing/collections/claims	31.1%	25.4%
System access record/access security	26.2%	22.4%
ROI tracking	25.7%	29.2%
Medical records/HIM/electronic health record	25.7%	23.1%
Compliance	21.5%	19.7%
Facility directory (of patients)	17.7%	19.3%
Appointments and/or scheduling	14.7%	11.5%
Master patient index or similar	14.3%	12.9%
Clinical functions	11.7%	7.1%
Admissions-transfers-discharge (or bed placement)	11.5%	9.5%
Order/entry system	11.1%	10.5%
Other	10.9%	9.5%
Ancillary systems such as: radiology/pharmacy/laboratories/etc.	8.5%	8.5%
Physician-related systems	8.1%	8.1%
Nursing-related systems	7.2%	7.8%
Emergency department	5.1%	6.8%
Social work	4.0%	3.1%
Research protocol tracking	2.8%	2.4%
Public relations	2.1%	2.7%

"All" represents 662 responses and "Hospitals" represents 369 responses.

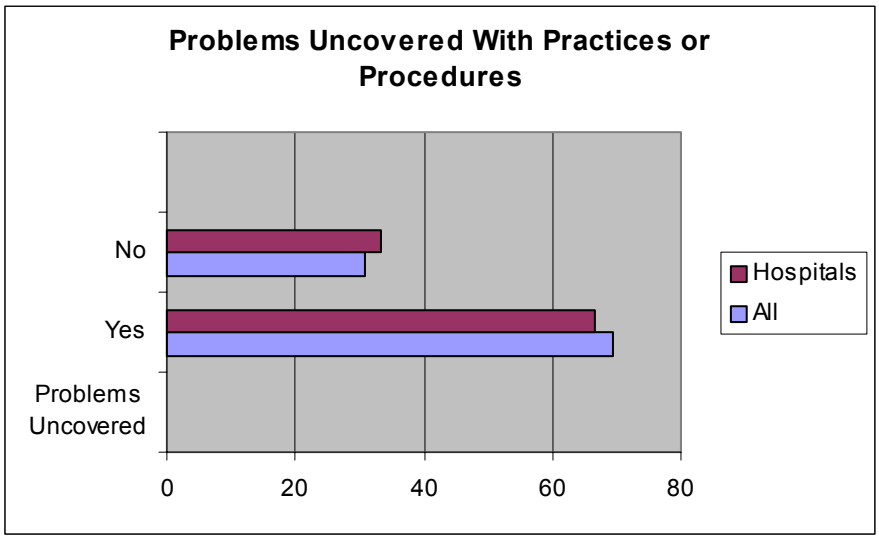
Again, just what software had to be revised or purchased greatly depended on the organization, size, and other systems changes that may or may not have been planned for the same time. It was not surprising to see that admissions software came in second at 31.1 percent. Given some admissions systems, this could actually be an even higher number since many systems combine some of the functions indicated in the chart above. Security access systems also place high (26.2 percent) reflecting some of the access rules initiated in the privacy rules and potentially in the security rule as well.

PROCESS IMPROVEMENT

*"I think that overall HIPAA's privacy regulations have made a big difference in the public's perception of privacy as well as heightening the awareness of healthcare providers about the seriousness of keeping health information private."--**Survey respondent***

Value-added Improvement

Early in the privacy rule implementation process, AHIMA members were reporting that implementation was also allowing their facility to address some internal process issues as well. These members were pleased by this "value added" activity associated with HIPAA implementation. So we asked, "**Was your facility's implementation of the HIPAA privacy requirement successful in uncovering any problems with your (then) business practices or procedures?"** Nearly seven of 10 respondents agreed that the HIPAA process helped to uncover problems with existing business practices or procedures.



Many comments, including comments from our previous internal AHIMA member survey in October 2003, noted that policies and procedures being addressed for privacy also resulted in some non-privacy changes as well. For example:[12]

- Numerous paper data sheets and reports (all with protected health information) processes have been reviewed—not only did health information become protected, but the entire process of moving data on paper has significantly improved
- Transcription and coding processes have been improved with regard to the security of the data and amount of turnaround time
- Implementation of the business associate process has engineered new policies and software that the entire business associate contract process has improved
- Sub-provider and subcontractor contracts have improved beyond privacy
- Improved data protection mechanisms have been added to systems
- Check-in and check-out procedures have improved
- Retention and destruction processes have been reviewed and improved

Process Improvement
Several questions were asked about the implementation process. An open-ended question was asked regarding the **number one problem implementers experienced in preparing their organizations to be HIPAA compliant.** Several problems were identified, but no single issue outside of accounting for disclosures was specifically addressed.

The most common identified issues included:

- **Awareness of Violations of Privacy/Public Conversations and Discussions:** As this issue was raised, most who reported it also indicated that once awareness was raised within the organization, the reaction was positive. They added that, at present, staff are much more compliant than ever before. This is a notable success.

- **Accounting for Disclosures:** This remains the number one issue raised by privacy officials. The ability to account and control disclosures varies by a facility's organization, size, and staff makeup. Separate from the accounting process was the initial identification of how much information was leaving an organization – in many cases for legitimate, but potentially (under HIPAA) questionable reasons. It was clear that many organizations spent considerable time addressing each of these issues and changing processes, policies, and procedures to address such releases conservatively (see "Amount of Information Shared").

- **Restricting Access to Protected Health Information:** Organizations take different approaches to this issue. Similarly, they need to address areas such as electronic

[12] "AHIMA Testimony to the National Committee on Vital and Health Statistics Privacy and Confidentiality Subcommittee." November 19, 2003. Available at www.ahima.org.

information, information that may have been displayed in public or semi-public areas of the facility, employee access, and clinical access. While many early detractors indicated that significant funds would be required to address this issue, it does not appear that this was the case. Unfortunately, it appears that most organizations did not keep track of the expenses incurred to address and resolve these various access issues. The HHS Office of Civil Rights did address many of the physical issues related to access on its Web site, which may have kept organizations from making unnecessary investments in building modifications and computer security. As the security rule is implemented and more work is done on the access issue, costs may change or may be better identified.

- **Amount of Information Shared/Appropriately Shared Information:** This was identified in several different ways. For some respondents this issue centered on the "minimum necessary" requirement of the rule. Some viewed this as an internal issue (how much information was being shared by internal personnel), others as intramural (how much information was being shared by professionals who practiced at the institution, e.g., medical staff/physician offices). Still others looked at this as an interested party issue (how much was or should be shared with individuals such caregivers, relatives, and clergy). Respondents did indicate that confusion remains on just which "relatives" can or cannot have access to all or some information regarding the patient.

- **Business Associate Agreements:** That business associate agreements are a source of confusion was not and should not be a surprise to many who have been involved with the rule. It is continually raised as an issue and an extension (April 14, 2004) was given for organizations to address various types of business associate agreements for resolution. From a process perspective, some of the problems with business associate agreements concern which officer in the organization was or is actively involved in the actual agreement and the number of agreements that might exist. This is an issue that requires attention in future years.

- **Faxing of PHI**: Many organizations indicated some confusion regarding faxed information and the process of faxing. It appears that most of these issues have been addressed, but this may be another issue that needs some attention, as well as information exchanged over the Internet.

- **Education:** A great variance among covered entities was identified. The HIPAA rule requires education of all staff and volunteers of an organization on the premise that everyone has some involvement with privacy. Members have noted, however, that HIPAA privacy education has extended to all sorts of other parties. Patients, patient caregivers, and relatives are obvious groups, but facilities have also had to "educate" non-healthcare members of the legal profession, law enforcement officers, court officers, clergy, and other providers.

- **Disposal of PHI:** Several commenters noted that many staff were not cognizant of the need to properly dispose of PHI contained on unofficial (scratch paper, temporary records, etc.) or official records.

Many comments did not fit neatly into the areas highlighted above. Some of these were also directed at specific types of providers, but not in numbers that could be construed as a trend. For instance, hospices noted a number of issues with the rule that do not apply to other providers. Facilities like nursing homes, behavioral health, and long-term care facilities note different issues because they interact more with patients' families than hospitals, clinics, physician offices, or health plans do. Responders from rural facilities also noted that the size of their communities made privacy a more difficult issue, given the day-to-day interaction between staff and patients (on the street) than large "impersonal" urban facilities.

Overall, many of the issues noted above also deal with change. Many of the respondents indicated that some of the challenges they faced were due to the change in existing practices and the introduction of new processes. This is different than problems with the rule itself, but a direct relationship exists between some parts of the rule and the challenges noted above. It will be necessary to address these lingering challenges in the coming years.

Staff Support

We asked a specific question with regard to the **general reaction of the facility's staff (patient care and related) to the changes made to implement HIPAA privacy.** Their response was:

Staff reaction to changes for HIPAA privacy	**All**	**Hospitals**
Very supportive of efforts to protect the privacy of their information	33.1%	32.7%
Somewhat supportive	47.7%	47.9%
Indifferent	8.1%	7.4%
Not very supportive	10.2%	11.3%
Not at all supportive	0.8%	0.8%

In total, more than 80 percent of respondents were supportive or very supportive. This is a welcome sign in comparison to predictions that provider staff would resist the changes. While the 10.2 percent reported a lack of support for change, this should not be a surprise for any organization going through a change as large as HIPAA privacy. Whether this same response will accompany the security changes remains to be seen, but we see this support as an excellent sign of commitment by healthcare professionals.

Patient Interaction

The privacy rule also had an impact on a provider or health plan's patients or participants. Most individuals were not impacted directly by HIPAA privacy requirements until the actual implementation. These same individuals were affected by:

- the rule itself
- by the entity's interpretation of the rule and the processes and procedures and notices implemented (changes)
- by other entities' implementation (hospitals/physicians/dentists/pharmacies/health plans) (also changes)

We asked respondents to give us their opinion on the ***initial*** **general reaction of their facility's patients to changes related to HIPAA privacy.** We also asked them for their ***current*** **general reaction of patients to changes related to HIPAA privacy.** Their response was:

Reactions to changes related to HIPAA privacy	**All/Initial**	**All/Current**
Very supportive of efforts to protect the privacy of their information	16.7%	22.0%
Somewhat supportive	22.7%	29.4%
Indifferent	38.8%	39.8%
Not very supportive	7.6%	5.5%
Not at all supportive	2.0%	.8%
Uninformed/Confused	12.2%	2.4%

The respondents ***initially*** felt that more than 20 percent of patients/subscribers were either uninformed/confused or not supportive of the HIPAA changes. The good news is that respondents now believe that after a full year of HIPAA compliance the number of uninformed/confused individuals has dropped to a very low percentage, 2.4 percent. In addition, respondents indicated their belief that those patients/participants who are supportive of the changes has grown from 40.4 percent to 51.4 percent. We believe that continued outreach from the Department of HHS, AHIMA, and other organizations will continue the upward trend of support for the privacy rule's changes.

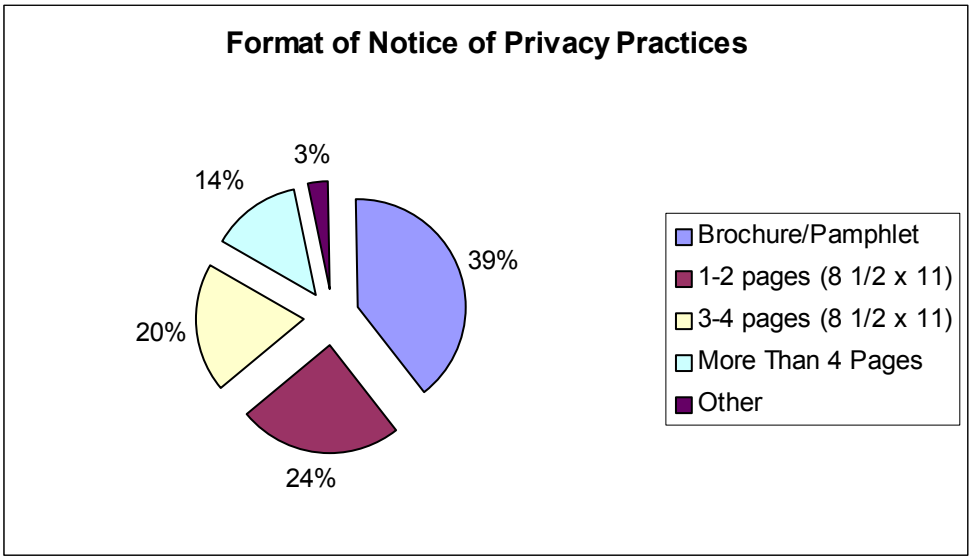
It would be beneficial for organizations to continue to monitor their patient/participant sentiment regarding the privacy rule and their concerns or lack of trust with the HIPAA requirements.

Notice of Privacy Practices

Another issue that received considerable negative feedback during the development of the HIPAA privacy rules was the notice of privacy practices. Many predicted notices of 20 or more pages in legal language that could be understood by few. Concerns were also raised as to how such notices could be delivered to patients and the costs of such delivery.

The AHIMA survey indicates that most notices are less than four pages (86 percent). Most are delivered in person rather than mailed or distributed in some other fashion. Thirteen percent of all respondents (14 percent of hospitals) indicate that they have revised their notice since it was initially presented.

One question asked **in what format the notice of privacy practice is presented to the patient.** Approximately 40 percent of the respondents' entities use a brochure or pamphlet to meet their notice requirement.



Other questions were:

Have you revised your notice since the initial notice was given out?

Revision of Notice	All	Hospitals
Yes	13.3%	14.2%
No	86.7%	85.8%

How are notices of privacy practices delivered to the inpatient?

Inpatient delivery method	All	Hospitals
Mail before admission	1.0%	0.6%
Mail after discharge	0.3%	0.0%
In person at admission or during admission	82.6%	98.3%
Not applicable	16.1%	1.1%

How are notices of privacy practices delivered to the outpatient?

Outpatient delivery method	All	Hospitals
Mail before initial or "next" visit	2.9%	1.1%
Mail after initial visit	0.3%	0.2%
In person at initial visit	83.5%	96.1%
Not applicable	13.3%	2.7%

How are notices of privacy practices delivered to the emergency patient?

Emergency patient delivery method	All	Hospitals
In person after services are rendered	63.4%	84.8%
Mailed after patient is discharged from ER/ED	2.5%	2.1%
Not applicable	34.1%	13.1%

Along with a requirement to deliver a notice of privacy practices to patients, HIPAA requires that each individual return an acknowledgement that the notice has been received. Respondents were asked to estimate **the percent of acknowledgement that their facility was experiencing.** The responses to that question were:

Estimated percent of returned "acknowledgement"	All	Hospitals
90 – 100%	74.7%	78.6%
70 – 89%	11.5%	10.1%
50 – 69%	2.1%	2.3%
Less than 50%	2.7%	1.4%
Do not know	9.1%	7.7%

Approximately three quarters of respondents indicate 90 to 100 percent return of acknowledgements for the notice. For the remaining 25 percent of respondents, we do not know why the acknowledgement is not received, since most are given in person. Additionally, we do not know the status and location of the patient/individual who did not return the acknowledgement. Whether or not this will be perceived as a problem will not be clear until either the complaint process or audits are completed in future years. The response rate bears attention by individual privacy officials to determine whether this number can be improved within their organizations.

Joint Notices

The HIPAA rule also allows facilities to join with individual physicians and physician groups in providing a joint notice of privacy practices. Such a joint effort would be expected in hospitals. The survey asked respondents to indicate the **percentage of the physicians practicing in their facility included in the notice.** Their response was:

Percent of Physicians Included	All	Hospitals
Less than 25%	21.6%	24.1%
25-50%	6.5%	9.0%
51-75%	4.2%	4.1%
More than 75%	67.7%	62.8%

68 percent of all respondents and 63 percent for hospitals indicated that the notice included more than 75 percent of the practicing physicians.

Many individuals first encountered the privacy rule in 2003-04. Beyond this first year of HIPAA privacy compliance, covered entities will need to revise and reissue their notices. Initially, organizations provided notices conscientiously to all individuals. Now that this initial distribution has been accomplished, covered entities will need to ensure that new patients receive the same attention and distribution as in the initial days of compliance. This will be an ongoing challenge for HIPAA privacy officials.

COMPLAINTS

HIPAA requires entities covered by the rule to respond to complaints. Given the amount of media attention paid to complaints about the privacy rule, we wanted to determine whether covered entities were receiving complaints from individuals. We did not want to determine a percentage of complaints, since many seem to result from general confusion about the rules. We also did not want to put respondents in a position of either ignoring this question or trying to determine legitimate complaints versus confusion. This is an area that needs some attention in the future; it is already being addressed by the Office of Civil Rights and some citizen groups.

The survey simply asked:

Has your facility received any complaints from individuals (patients) regarding the HIPAA rule or their rights [under the HIPAA rule]? The response was:

Complaints	All	Hospitals
Yes	53.8%	61.4%
No	46.2%	38.6%

The data does not indicate whether there are multiple complaints or just one. In hospitals, complaints did appear to increase slightly as facility size increased.

PROBLEMS WITH THE HIPAA RULE

"I feel our health system did a very good job in getting ready for HIPAA. There remains confusion, though, with staff on topics such as business associates, research, and when to account for disclosures." ***--Survey respondent***

We asked for a specific response to problems perceived with the HIPAA privacy rule as opposed to change and challenges. The categories listed were broken down by sections of the rule and some of the problems that had been identified in previous AHIMA surveys and November 2003 NCVHS testimony.

We asked: **Is your facility experiencing any problems with the requirements or processes listed below:**

Privacy Rule Requirements	**All**	**Hospitals**
Accounting for release of protected health information	38.6%	39.3%
Obtaining protected health information from other providers	33.3%	29.5%
Access and release of information to relatives or "significant others"	31.6%	31.8%
Business associate requirements	24.5%	22.4%
Confusion by individuals/patients in understanding the notice of privacy practices	24.2%	22.6%
Access and release of information to law enforcement	21.6%	25.2%
State preemption requirements related to consents needed for release of information covered under treatment, payment and/or healthcare operations	18.0%	16.4%
Release of information (post care) to patients and/or their representatives	17.3%	18.2%
Access and release of information for subpoenas versus court orders	15.3%	17.8%
The directory process (not related to clergy)	14.9%	18.8%
The authorization process	14.5%	13.1%
Release of information to clergy ("directory" requirements)	11.1%	14.2%
Access to or release of information under research protocols	11.0%	9.9%
The de-identification processes	10.1%	9.6%
Access and release of information for public health requests	7.6%	8.0%
Providing the notice of privacy practices	5.9%	4.2%
Access and release of information to the media/press	5.1%	6.0%

Accounting for release of PHI ranked highest at just below 40 percent. Other items that scored above the 30 percent mark were **access and release of information to relatives and significant others** and **obtaining PHI from other providers**. These responses mirror anecdotal information AHIMA has collected from the industry as well as some of the complaints reported by industry media.

Just under a quarter of respondents also identified problems with the **notice of privacy practices** and **business associate requirements.** The data does not indicate whether the problem was due to the way the entity implemented the requirement or whether it was the

requirement itself. Both of these requirements address items that can vary greatly due to factors affecting a specific entity. It is clear from other responses that many organizations have subsequently changed their notice of privacy practices. Since the compliance date for various business associate agreements is just upon us, we may not know the significance of this problem until 2005.

Three of the high responses–**access and release of information to law enforcement, access and release of information to relatives or "significant others," and obtaining PHI from other providers**--may be due to preemption issues. Many commented that state requirements made these issues a problem. The Office of Civil Rights has reported to the NCVHS that some complaints have turned out not to be HIPAA issues but rather state issues.

Degree of Difficulty

To get a better picture of the problems noted above, we asked each respondent who answered "yes" to a particular "problem" to also respond to the "amount of difficulty you are having with each requirement." A scale of difficulty was provided with "slight difficulty" being scored as a 1, "moderate difficulty" a 3, and "extreme difficulty" scored as a 5. The results of this question were:

Privacy Rule Requirement	**All (mean)**	**Hospitals (mean)**
Accounting for release of protected health information	3.22	3.24
Business associate requirements	2.99	3.02
Access to or release of information under research protocols	2.98	2.95
The de-identification processes	2.97	3.16
Access and release of information for subpoenas versus court orders.	2.97	2.87
State preemption requirements related to consents needed for release of information covered under treatment, payment and/or healthcare operations	2.93	2.97
Obtaining protected health information from other providers	2.86	2.85
Access and release of information to relatives or "significant others"	2.86	2.83
Access and release of information to law enforcement	2.75	2.71
Access and release of information to the media/press	2.62	2.60
The authorization process	2.58	2.52
Confusion by individuals/patients in understanding the notice of privacy practices	2.56	2.68
Release of information to clergy ("directory" requirements)	2.55	2.65
The directory process (not related to clergy)	2.53	2.54
Access and release of information for public health requests	2.52	2.55
Release of information (post care) to patients and/or their representatives	2.45	2.50
Providing the notice of privacy practices	2.11	2.07

The level of difficulty reported by respondents overall was between slightly difficult and moderately difficult. The only exception was **accounting for release of PHI,** which was rated slightly above moderately difficult.

Next we asked the respondents about areas of the rule that they **believed needed to be modified by the federal government.** The response was:

Privacy Rule Requirement	**All**	**Hospitals**
Accounting for release of protected health information	50.5%	55.7%
No further modifications at this time	24.8%	21.2%
Business associate requirements	19.8%	18.7%
Access and release of information to relatives or "significant others"	17.8%	17.6%
Content of notice of privacy practices	13.2%	12.7%
Release of information to law enforcement	12.5%	13.4%
Release of information for subpoenas versus court orders	12.4%	13.4%
Authorization process	12.4%	11.4%
Providing the notice of privacy practices	12.3%	13.7%
De-identification process	9.8%	10.8%
Release of information (post care) to patients and/or their representatives	9.3%	9.6%
Exclusion of a consent for treatment, payment and healthcare operations	8.6%	7.2%
Access to or release of information under research protocols	8.4%	7.8%
Release of information to clergy ("directory" requirements)	8.2%	9.6%
Access to patient records for initial identification of patients for research studies	8.1%	7.5%
Access and release of information for public health requests	7.6%	7.7%
Director process (not related to clergy)	5.2%	5.9%
Access and release of information to the media/press	2.3%	2.1%

No surprise that the requirement for **accounting for release** was most often mentioned by those responding–50 percent (All) and 55.7 percent (Hospitals). Twenty-five percent of those responding indicated that no modifications were needed at this time.

There were several categories above 10 percent, certainly too low to suggest an immediate need to consider change. But these items deserve further attention from both policymakers and covered entities. These include several requirements receiving responses between 10 and 20 percent, which collectively might be pointing to issues associated with **state preemption**. And **business associate agreements** (19.8 percent) might warrant attention once their compliance date is reached and more specifics can be gathered.

Requests for an Accounting of Release of Protected Health Information

Since the requirement of accounting for release is most often raised as an issue by covered entities and privacy officials, we asked respondents how many times their facility had been asked for an accounting.

Number of requests for an accounting since April 14, 2003	All	Hospitals
0	71.7%	75.2%
1-2	13.0%	12.3%
3-4	3.6%	3.3%
5-10	2.2%	1.5%
11-15	0.3%	0.2%
More than 15	2.7%	2.4%
Don't know	6.5%	5.1%

In total, 72 percent of respondents (75 percent in hospitals) reported that they have not received a single request for an accounting for release of protected health information, with just three percent reporting more than 15 such requests. AHIMA and others have testified to the NCVHS that the accounting rule should be modified to eliminate most accounting and find another way for individuals to be aware of releases required by law. To date, this response would indicate that such a modification should be strongly considered.

Consent

Prior to implementation and even before the HIPAA privacy requirements were finalized, there was considerable debate as to whether covered entities should be required to obtain a consent for the release of information for the purposes identified in the rule as "treatment," "payment," and "healthcare operations" (TPO). The final rule for HIPAA privacy made the use of such a consent optional.

While such a consent is optional under HIPAA, some states specifically require a consent. Since HIPAA does not completely preempt state law, the consent is therefore required of the covered entities in the states with such a requirement. Two questions were asked regarding TPO consents.

First, we asked if the respondent's **state required a patient consent for the disclosure of PHI for treatment, payment, and healthcare operations.**

Consent for TPO Required by State?	All	Hospitals
Yes	34.2%	31.2%
No	53.2%	57.2%
Don't know	12.6%	11.6%

Approximately one third of those responding indicate a state consent requirement. We are concerned, however, that more than 10 percent of those responding to the question did not know their state's requirement.

The second question asked **whether the facility requests patient consent for the disclosure of PHI for treatment, payment, and healthcare operations.**

Consent requested by the facility	All	Hospitals
Yes	51.5%	51.5%
No	45.2%	46.5%
Don't know	3.3%	2.0%

While one third of the entities report a state requirement, over half of the respondents indicate that they are requesting a consent. This may be because of the difficulty reported in receiving information from other providers or certain state entities. Objections to the use of consent forms were mainly due to the administrative problems surrounding them at the time the HIPAA final rule was introduced. Whether these concerns have changed since then is unclear. For hospitals, the size of the institution did not appear to impact the percentage that were using a TPO consent process.

PRIVACY TRAINING

"One good thing was increased education of staff to heighten awareness of releasing patient information." ***--Survey respondent***

AHIMA was interested in seeing how covered entities approached the training requirements of the rule, given the diverse groups that required training. Several questions were asked and the responses may be helpful as organizations address ongoing privacy orientation and retraining.

Respondents were asked **how they addressed medical staff training**:

Type of Instruction for Medical Staff	All	Hospitals
In-house instruction by privacy officer/education officer	59.5%	60.2%
In-house instruction by external consultant/trainer	6.1%	7.2%
In-house instruction by facility counsel (attorney)	3.4%	4.5%
Instruction external to the facility	3.2%	3.5%
Video instruction developed by the facility/system	4.7%	4.5%
Video instruction bought from an external source	3.4%	4.1%
Web-based instruction developed by the facility/system	8.7%	7.2%
Web-based instruction bought from an external source	5.0%	5.3%
Not applicable	5.9%	3.5%

In six of 10 cases, training was completed by an internal privacy official or education staff. Web-based training was used 14 percent of the time, with more of such instruction developed internally.

Respondents were asked **how they addressed training for general staff <u>not</u> required to fulfill specific PHI or HIPAA functions related to PHI:**

Type of Instruction for General Staff	All	Hospitals
In-house instruction by privacy officer/education officer	56.6%	56.9%
In-house instruction by external consultant/trainer	2.3%	2.6%
In-house instruction by facility counsel (attorney)	0.7%	0.3%
Instruction external to the facility	0.6%	0.5%
Video instruction developed by the facility/system	6.7%	6.8%
Video instruction bought from an external source	6.7%	7.8%
Web-based instruction developed by the facility/system	9.2%	8.7%
Web-based instruction bought from an external source	5.3%	5.4%
Not applicable	9.9%	9.0%

Again, approximately six of 10 entities provided internal instruction, with a slight increase in the amount of Web- and video-based instruction. The amount of non-applicable numbers is potentially higher, because many small entities have smaller numbers of "general" staff–most staff are directly involved in PHI. This might also account for the increase in "machine"-based education.

Respondents were asked **how they addressed training for staff required to fulfill specific PHI or HIPAA functions:**

Type of Instruction for PHI/HIPAA Function Staff	All	Hospitals
In-house instruction by privacy officer/education officer	68.5%	68.5%
In-house instruction by external consultant/trainer	2.9%	2.9%
In-house instruction by facility counsel (attorney)	0.9%	0.9%
Instruction external to the facility	1.1%	0.8%
Video instruction developed by the facility/system	5.5%	5.3%
Video instruction bought from an external source	3.8%	4.5%
Web-based instruction developed by the facility/system	9.1%	8.9%
Web-based instruction bought from an external source	7.0%	7.7%
Not applicable	1.3%	0.6%

We did not believe it was surprising that the percentage of internal instructors increased in this area to approximately 70 percent. Much of this instruction also had to be applied to specific processes and areas of various facilities. This would also account for an even higher (9.1 percent) amount of Web-based instruction that can address different functions and positions and is probably more cost-effective in larger organizations.

Volunteer training:

Type of Instruction for Volunteers	All	Hospitals
In-house instruction by privacy officer/education officer	58.5%	64.3%
In-house instruction by external consultant/trainer	2.0%	2.9%
In-house instruction by facility counsel (attorney)	0.2%	0.0%
Instruction external to the facility	0.5%	0.5%
Video instruction developed by the facility/system	9.1%	10.2%
Video instruction bought from an external source	4.8%	5.7%
Web-based instruction developed by the facility/system	6.8%	5.9%
Web-based instruction bought from an external source	3.4%	3.5%
Not applicable	14.8%	7.1%

HIPAA also requires that volunteers in covered entities be given privacy training. Under this category the frequency of internal personal instruction drops, mainly because many healthcare providers do not have such volunteers and where a number of institutions directed volunteers to video instruction (10.2 percent in hospitals) or Web-based instruction, where instruction can be more generalized.

As noted above, training is not a one-time event and these numbers will probably change as entities introduce new security procedures and update staff and volunteers on privacy requirements.

COSTS OF COMPLIANCE

*"HIPAA is all common-sense best practice and although some may question its cost, it is surely a great refresher in privacy."--**Survey respondent***

We were concerned about asking questions about the cost of HIPAA implementation mainly because we knew that many organizations did not prepare a recognized budget item for HIPAA privacy implementation. Rather, they tended to let costs fall in the departments that might be affected by any staff time or resource used as they addressed HIPAA.

A second difficulty to determining costs was the extensive use of staff time for HIPAA implementation as opposed to tangible resources. The writing or revisions of policy and procedures, privacy notices, strategic planning, and education design all tended to be mainly personnel (salary and benefit) costs. Most healthcare organizations did not segregate time into various projects unless they hired an outside party to perform such a task. Third, budget years run in different cycles (i.e. January through December, July through June, or October through September). Depending on when implementation efforts were initiated, they may or may not have been identified in the budget year being reported.

Finally, our questions were asked after implementation had begun. We did not ask organizations to track this data, so the ability to identify it was limited. The best way to

capture cost data is to plan to collect such data from the outset, and it was clear that many organizations did not take such a step, although cost was a major objection from opponents of the privacy rule.

The survey, therefore, asked respondents to indicate the **size of their <u>current budget</u> for HIPAA privacy compliance**. The results were:

Size of Budget	**All**	**Hospitals**
No budget	33.6%	35.1%
Over $200,000	4.1%	3.0%
$100,000 – 199,999	3.9%	3.5%
$75,000 – 99,999	2.4%	2.7%
$50,000 – 74,999	2.8%	2.4%
$30,000 – 49,999	2.1%	2.1%
$20,000 – 29,999	2.6%	2.4%
$10,000 – 19,999	2.8%	3.2%
$5,000 – 9,999	3.4%	3.9%
$1,000 – 4,999	5.8%	6.3%
$500 – 999	1.4%	1.5%
Less than $500	3.4%	2.3%
Unsure	31.6%	31.6%

One third of those responding did not indicate a separate budget for HIPAA privacy. Another group, slightly less than one third, indicated that they were unsure of the size of the budget. Given that the questions were asked in February 2004, we assume that most if not all organizations reporting are citing post-implementation/ongoing compliance costs that may reflect personnel costs for privacy officials, software costs if not fully implemented, and so forth. The fact that almost one third indicated "unsure" may also mean that compliance has been buried in the cost of doing business and is not worth dealing with as a separate issue. In the future, if such costs are considered important to our understanding of privacy, confidentiality, and security, financial and personnel questions will need to be raised early enough for organizations to trace them.

Many organizations predicted implementation and maintenance costs in the millions for covered entities. **Nothing in the responses to this survey and in previous surveys and questions from AHIMA would indicate that the costs came anywhere near these predicted amounts.** That is not to say that privacy officials, committees, and the staffs and volunteers of various entities did not put in many long hours to contribute to the implementation of HIPAA. Clearly, a significant effort was put forth in time that translates to salaries, benefits, other resources such as software, printing, and educational materials as well as lost opportunities or revenue-producing activities that could have been pursued in the absence of this mandate. Even so, few organizations have come forward to say that these efforts caused them financial distress.

As HIPAA privacy moves forward, it would help to know the costs and benefits associated with compliance, since, as pointed out above, there are also cost savings

encountered. In the future we hope organizations will consider tracking costs and budgets related to privacy rule compliance.

THE HIPAA SECURITY RULE

The HIPAA security rule places security as a subset of the privacy requirement. In a sense, security relates to electronic protected health information and to the general physical safety of all protected health information. Since the first anniversary of HIPAA privacy compliance essentially marks the halfway point for the HIPAA security compliance date (April 21, 2005), we asked some initial questions of these same covered entities regarding their HIPAA security implementation.

Our first questions concerned **whether or not the organization has established a committee or task force to address the implementation of the HIPAA security rule.** 82 percent of the respondents answered "yes" (85.7 percent for hospitals), slightly less than the responses we received with regard to similar committees or task forces for privacy. Individual responses would seem to indicate that some presume that security is an information technology function and not a cross-departmental activity. This raises some concerns. While the regulations do address many information technology issues, there are policies and procedures that will need attention. The manner in which HHS presented the security requirements and the unique qualifications of HIM professionals both speak to a need for HIM professionals to be involved in security compliance. Some respondents did indicate that they believed they had already met the requirements for security and did not need to address them further.

The HIPAA security rule also recommends an individual be placed in charge of the security requirements. 80 percent of those responding indicated that this has been done. When asked **what position fulfills this requirement in their organization, the response was:**

Position Fulfilling the Security Officer Function	All	Hospitals
HIM/Medical Record Dir/Mgr	7.6%	5.6%
Compliance officer	7.7%	6.8%
Risk manager	2.3%	3.0%
Privacy officer	6.7%	7.2%
CIO	7.8%	8.9%
IS or IT personnel (Director/Mgr)	56.9%	59.9%
Other	10.9%	8.7%

The results clearly show the security position has fallen to the organizations' CIO or IT personnel, with responses of some 64 percent (All) and almost 69 percent (Hospitals). As with the privacy official position, many small organizations do not have an identified IS or IT department or individual, and we suspect that the function is being carried out by many of the same individuals identified for privacy. Many organizations also outsource their IT department and thus identification of the responsibility will vary.

Conclusion

"The impact of HIPAA has heightened respect for patient protected health information. I would like to see security have the same effect as privacy did: national attention for patients' rights under federal scrutiny."

Survey respondent

So where does the healthcare industry stand with HIPAA now—one year after implementation?

AHIMA's survey to assess the current state of HIPAA privacy within the healthcare industry indicates that as we bridge the one-year anniversary of the implementation of the HIPAA final privacy rule, the message from the industry regarding HIPAA privacy and security is a positive one:

- **The majority of facilities are significantly compliant.** While most are still striving to achieve total compliance, there still seem to be a few problem areas identified within the compliance requirements, led by accounting for release of protected health information.
- The privacy rule has helped a majority of organizations **identify where policies and procedures need improvement** in order to ensure the privacy of protected health information. The majority of staff and patients are supportive of new privacy policies and procedures.
- Implementation and compliance has been achieved primarily through the use of **existing staff and resources**, illustrating that the HIPAA privacy rule has not been the overwhelming burden to the healthcare industry that was predicted by opponents of the privacy rule.
- **There is more work to be done**. Survey respondents indicate that some areas should be addressed for modification.

AHIMA is pleased with the results of this initial survey. We look forward to continuing this effort annually to gauge the status of HIPAA privacy implementation. Over the coming months, we will further assess our survey results and methodologies in preparation for future surveys. We will also look for additional opportunities to expand the scope and reach of our analysis.