



The Value of HIM in Privacy and Security Compliance

by Margret Amatayakul, RHIA, CHPS, CPHIT, CPEHR, FHIMSS, and Mitch Work

Survey results illustrate HIM participation in compliance efforts and offer a look at common program components

HIM professionals have long been at the forefront of ensuring the privacy and confidentiality of health information. With the introduction of the HIPAA privacy and security rules, this work took a challenging new focus as organizations covered by the law worked to meet its requirements.

A closer look at how HIM professionals participate in organization efforts offers a measure of the HIM value in privacy and security compliance efforts as well as common program characteristics.

In January 2006 AHIMA surveyed members about the progress of their organizations' privacy and security compliance efforts. The association's Foundation of Research and Education (FORE) added a component surveying HIM participation in these efforts. The results clearly indicate that HIM professionals make major contributions.

There are several especially strong indicators that suggest HIM's importance to HIPAA privacy and security compliance:

- Hospitals value credentialed information privacy officials. Respondents indicated that approximately 31 percent of hospitals required AHIMA's RHIA or RHIT credential. Another 14 percent required an additional specialty credential relating to healthcare privacy, and 6 percent required a specialty credential without the RHIA or RHIT. Hence fully 51 percent of hospitals require some credential for their information privacy official.
- HIM professionals play prominent roles in HIPAA privacy and security steering committees or teams, serving as chair or member in 90 percent of such groups.
- Collaboration between a facility's information privacy and information security officials appears to be an important factor, and several respondents indicated the lack of such collaboration was a barrier to full compliance. Results indicate that collaboration in some form occurs in 90 percent of hospitals.

A formal process to assess compliance appears to be a key ingredient of successful compliance programs. Fully 75 percent of the hospital respondents indicated they assess privacy compliance. Assessment is highly characteristic of those organizations who report higher levels of compliance (see the figure "Assessment and Compliance").

Assessment and Compliance

Organizations that report higher levels of privacy compliance are very likely to have formal compliance assessment programs.



p>.0001

Of the 832 organizations that assess privacy compliance, almost 62 percent indicated they had received a **complaint** (p>.00001). Organizations that had experienced **complaints** were likely to use a formal assessment process as part of their remediation.

The survey also sought to categorize the types of formal **complaints** organizations are receiving and how HIM professionals responded. The most common were disclosure and other release of information issues and breach of confidentiality, as shown in the table, “The Nature of **Complaints**,” which summarizes the results from an open-ended question.

The Nature of **Complaints**

Respondents report a range of consumer **complaints**, summarized here from an open-ended question. Behind many were human factors, such as lack of time or focus by staff and misunderstanding of privacy rights by the public.

Nature of Complaint	% of Respondents
Unauthorized disclosures and other release of information issues	19
Breach of confidentiality (intentional and unintentional)	18
Missing protected health information	11
Release of information to wrong person, lab, physician, other	8
Disclosures to family (incorrect, correct, and insufficient)	7
Privacy concerns in general	6
Communication problems stemming from physicians	5
Password sharing, access controls, and other security issues	5
Misunderstanding of the rules (by patients and staff)	4
Issues associated with amendments	4
Interference with patient requests for access, timeliness issues	4
Voicemail, e-mail, and fax issues	2
Open or unattended records, folders, papers, schedules, etc.	1
Improperly disposed of protected health information	1

Patients protesting required disclosures	1
Facility directory issues	1
Issues with copy fees	1
Identity theft (patient and physician)	1
Other or vague response	3

n = 639; total does not equal 100 percent due to rounding

A key contributor to **complaints** might be best described as the human factor. Many respondents suggested that healthcare professionals, and in particular physicians, as well as other members of the work force did not have the time or focus to ensure that all matters of privacy and security are always addressed.

Some aspects of the human factor, however, are very much related to the level of understanding about HIPAA privacy and security on the part of the public. **Complaints** about correct disclosures to family along with patients protesting required disclosures clearly suggest that education is still very much needed. This is clearly a role for HIM professionals.

Hospitals and health systems generally respond to **complaints** in several ways. The table “Common Responses to **Complaints**” illustrates how those who reported receiving formal **complaints** responded to them. Training, mitigation, providing requested information, and policy and procedure revision are almost always performed.

Common Responses to **Complaints**

Organizations report a variety of responses to formal **complaints**, with increased work force training being the most common.

Response to Complaint	% of Respondents
Enhance work force training	27
Take steps to mitigate the effects of any violation	24
Supply written or verbal information requested	23
Revise policies and procedures	20
Institute formal, internal assessment process	5
Employ third party to conduct formal assessment process	1

n = 288

This survey and other indicators suggest that compliance with the HIPAA privacy and security rules may become an uphill battle after an initial surge to become compliant.

HIM professionals have always played a critical role in protecting patient privacy. It is now incumbent upon them to ensure that such protections are expanded into electronic systems within their facilities and to health information exchanges. The challenges faced today will only grow exponentially with the exchange of health information through regional and nationwide health information networks.

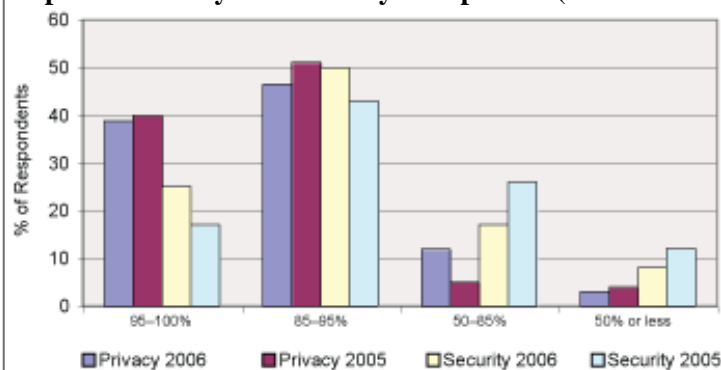
The State of Compliance

Self-reported compliance with HIPAA privacy and security rules has remained relatively steady in the past two years. Respondents to AHIMA's 2006 HIPAA privacy and security compliance survey noted a slight slip in privacy compliance and modest gains in security.

A total of 1,117 AHIMA members working in hospitals and health systems participated in the survey. Nearly 40 percent reported their facilities were in full compliance with the privacy rule (defined as 95 to 100 percent compliant). That share remained virtually the same from 2005. There was a drop in 2006 of about 6 percentage points in those reporting privacy compliance at the 85 to 95 percent level. Respondents report less compliance with security overall, although there has been an increase since 2005 (7 percentage points at both the 95 to 100 percent and 85 to 95 percent compliant levels).

Respondents identified a number of significant barriers to full privacy compliance. Lack of staff training and appreciation for compliance needs were identified by more than 40 percent of respondents. Other barriers, accounting for another 50 percent of the responses, included lack of time or staffing, controls, funding, and administrative support. The remaining 10 percent of respondents cited barriers including too many rules, changes in the rules, state pre-emption issues, and lack of patient understanding.

Reported Privacy and Security Compliance (2005 and 2006)



Source: AHIMA. "The State of HIPAA Privacy and Security Compliance 2006." April 2006. Available online at (www.ahima.org).

Margret Amatayakul (margret@margret-a.com) is president of Margret\A Consulting, LLC, based in Schaumburg, IL. **Mitch Work** (mitchwork@workgroupinc.net) is president of the Work Group, Inc., based in Lincolnshire, IL.

Article citation:

Amatayakul, Margret; Work, Mitch. "The Value of HIM in Privacy and Security Compliance." *Journal of AHIMA* 78, no.5 (May 2007): 44-46.

Copyright ©2007 American Health Information Management Association. All rights reserved. All contents, including images and graphics, on this Web site are copyrighted by AHIMA unless otherwise noted. You must obtain permission to reproduce any information, graphics, or images from this site. You do not need to obtain permission to cite, reference, or briefly quote this material as long as proper citation of the source of the information is made. Please contact Publications at permissions@ahima.org to obtain permission. Please include the title and URL of the content you wish to reprint in your request.