CIOs’ Views of HIPAA Security Rule Implementation—An Application of Q-methodology

Mei Ao, MD, MS, and Rosemary Walker, DDS, MBA, MS

ABSTRACT

The purpose of this study is to uncover the attitudes held by chief information officers (CIOs) regarding the implementation of HIPAA’s Security Rule. In March and April of 2004, five Chicago area CIOs were surveyed and asked to rank 26 opinion statements that presented possible implementation barriers to the Security Rule. Q-methodology, which is a powerful tool in subjective study, was employed to identify and categorize the viewpoints of CIOs toward the barriers.

Two factors (opinion types) that represented two different views—socially motivated CIOs and resources-motivated CIOs—regarding the implementation barriers were extracted.

The study sheds light on the attitudes and perceptions of CIOs as they begin rule implementation. Current CIOs can use this information as a way to begin to examine what the prevailing attitude may be at their institution and, therefore, how to begin building a successful implementation strategy.

KEYWORDS

- HIPAA (Health Insurance Portability and Accountability Act)
- Security Rule
- Implementation
- Chief Information Officer
- Human behavior
- Resources
- Q-methodology

Introduction

In 2003, the Security Final Rule was published in the February 20 Federal Register with an effective date of April 21, 2003. Covered entities, with the exception of small health plans, have until April 21, 2005, to comply with the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. HIPAA outlines three groups that qualify as covered entities: health plans, healthcare clearinghouses, and healthcare providers. The security rule ensures a minimum level of security so that electronic protected health information, or EPHI, remains private. It outlines a broadly flexible model for security management across the healthcare industry.

Implementing the rule is challenging because covered healthcare organizations must identify and manage multiple barriers. The rule provides explanations of specifications rather than actual implementation guidelines. While there are other good resources that fully explain the rule, their...
effects on the implementation are limited because they more or less repeat the rule itself.

The security rule looms as a large concern for chief information officers (CIOs) at healthcare organizations. CIOs are increasingly present at the strategic planning level because of their expanded responsibilities. CIOs are becoming high-profile change agents, communicating and managing institutional changes driven by the forces of information technology.5 Because of the shift from administrative or billing systems to clinical information systems, CIOs need to have a different mix of skills and experience. Besides financial and technical skills, CIOs need to have the skills and knowledge to communicate with clinicians. In addition, they need to be able to manage the expectations of clinicians to ensure that they do not become unrealistic.6 Many CIOs choose to sponsor infrastructure issues that can affect the whole organization, including compliance with patient information confidentiality regulations required by HIPAA.7

The purpose of the research reported in this article is to uncover the opinions held by CIOs regarding the security rule implementation that may help other healthcare organizations with implementation strategic planning. A statistical technique called Q-methodology was used in this study. Q-methodology is a powerful tool used to analyze opinions, perceptions and attitudes in an objective way. The major concern of Q-methodology is not with how many people believe something, but with why and how they believe what they do.8 Q-methodology typically employs small numbers of respondents, and the in-depth study of single cases is not uncommon.9

Methods

Q-methodology was first introduced by psychologist/physicist William Stephenson in 1935. It is the combination of qualitative and quantitative research techniques that permits the systematic study of subjectivity.10 Q-methodology uncoveres and identifies the range of opinions regarding a specific topic under investigation, and it identifies groups of individuals with similar viewpoints.8

Research employing Q-methodology consists of three steps. First, a “concourse” is developed, which is usually a collection of statements or opinions that are related to a particular topic. From this concourse, a subset of statements, called the Q-sample, is drawn for administration in a Q-sort. Second, participants are asked to sort the statements along a continuum from “most agree” at one end to “most disagree” at the other, an operation referred to as “Q-sorting.” The third step is analyzing and interpreting the results of the Q-sorting.

Data analysis follows the Q-sorting. It includes Pearson’s correlation coefficient, factor analysis, and factor rotation. The correlation coefficient between two sorters indicates the extent to which their viewpoints are similarly expressed by the Q-sorts. The inter-correlation matrix of Q-sorts is then subjected to by-person factor analysis. The factor analysis procedure identifies groups of individuals with similar viewpoints11 Factor rotation enables researchers to look at other possibilities for grouping. QMethod software, available without charge, is tailored to the requirements of Q-methodology studies; it performs factor analysis and factor rotation.12

For this study, a list of possible implementation barriers was created based on a literature review and input from hospital and academic professionals with extensive HIPAA knowledge. From the list of barriers, 26 statements were selected as the Q-sample.

Before data analysis, each participant’s ranked and ordered statements were transformed into an array of numerical data as shown at the top of the grid in Figure 1. Before data analysis, each participant’s ranked and ordered statements were transformed into an array of numerical data as shown at the top of the grid in Figure 1.
In this study, the one statement that was placed at the Most Significant end of the distribution received a score of +4, the next two scores received +3, the next three scores received +2, and so forth, all the way down to the one statement that was found Least Significant, which received -4. Statements placed in the middle of the bell-shaped curve by the subjects are assigned scores of 0, meaning the CIOs were neutral regarding these statements.

Each participant’s array of numerical data then was intercorrelated with the arrays of all the others. The resulting correlation matrix shows which participants sorted the statements into similar orders. The correlation matrix is then subjected to factor analysis to obtain groupings of data arrays that are highly correlated. A factor emerges when enough people sort in a sufficiently similar way to represent a type of “group thinking.” The researcher then assigns a working name to each point of view.

### Results

Q-sorts were collected from five Chicago area CIOs from academic medical centers and integrated delivery systems in March and April of 2004. PQmethod 2.11 was used for data analysis.

Following the guidelines for Q-factor analysis, a correlation matrix was first obtained, as shown in Table 1. By-person factor analysis and QROTATE—the procedure that is used to manually flag defining sorts—extracted two factors, or opinion types, that represented two different views regarding the implementation barriers. Table 2 shows the factor matrix with an X indicating a defining sort, in which the participant’s statement array is highly correlated with a factor. The two opinion types were socially motivated CIOs and resources-motivated CIOs. Table 3 shows the statement scores by factors/opinion type. The characterizing statements of these two factors are shown in Table 4 and 5, respectively.

#### Socially Motivated CIOs

This factor was named “socially motivated CIOs.” Their responses indicated that individuals’ behaviors created the most significant barriers. Characterizing statements are listed in Table 4. They were concerned with...
employees’ behavior: clinicians can copy PHI (protected health information) and paste to their own files (statement 20, +3); handheld devices can cause security problems (statement 22, +2); employees can print PHI from insecure printers (statement 19, +2); and inappropriate employee access authorization (statement 11, +1). This factor considered co-existing manual and electronic patient medical records as the most significant barrier (statement 25, +4). This is not a short-term problem because it is difficult for healthcare organizations to switch to a paperless environment quickly. Better coordination and more cooperation among employees are needed for co-existing manual and electronic patient medical records. The factor indicated people’s behaviors might add more potential security risks caused by co-existing patient medical records.

This factor did not worry about choosing outside consultants (statement 15, -4), nor were they concerned with vendors or trading partners (statement 26, -2). They thought that a complex organizational/governance structure was not a significant barrier (statement 6, -3). They did not believe that new or revised policies and procedures would be inconvenient for workforce members (statement 10, -3).

This factor considered the following statements as neutral, meaning they did not feel strongly one way or the other about a statement: inadequate funds/budget for implementing changes (statement 4, 0); the organizational culture will be resistant (statement 5, 0); lack of potent password management policies/procedures (statement 13, 0); remote access can bring potential security problems (statement 14, 0); and inadequate funds/budget for implementing changes (statement 23, 0)

<table>
<thead>
<tr>
<th>Characterizing Statements</th>
<th>Scores</th>
</tr>
</thead>
<tbody>
<tr>
<td>Significant Barriers</td>
<td></td>
</tr>
<tr>
<td>Co-existing manual and electronic patient medical records.</td>
<td>4</td>
</tr>
<tr>
<td>Inadequate staff to implement changes.</td>
<td>3</td>
</tr>
<tr>
<td>Clinicians can copy PHI and paste to their own files.</td>
<td>3</td>
</tr>
<tr>
<td>Handheld devices can cause security problems.</td>
<td>2</td>
</tr>
<tr>
<td>Employees can print PHI from insecure printers.</td>
<td>2</td>
</tr>
<tr>
<td>Neutral</td>
<td></td>
</tr>
<tr>
<td>Remote access can bring potential security problems.</td>
<td>0</td>
</tr>
<tr>
<td>Loading of local applications to store or process PHI.</td>
<td>0</td>
</tr>
<tr>
<td>Outdated information technology.</td>
<td>0</td>
</tr>
<tr>
<td>Lack of potent password management policies/procedures.</td>
<td>0</td>
</tr>
<tr>
<td>The organizational culture will be resistant to it.</td>
<td>0</td>
</tr>
<tr>
<td>Inadequate funds/budget for implementing changes.</td>
<td>0</td>
</tr>
<tr>
<td>Insignificant Barriers</td>
<td></td>
</tr>
<tr>
<td>Some LANs are outside the control of the hospital’s IT department.</td>
<td>-2</td>
</tr>
<tr>
<td>Vendors and trading partners are unaware of HIPAA regulations.</td>
<td>-2</td>
</tr>
<tr>
<td>Insufficient policies/procedures regarding system access by non-employees, i.e. Physicians of affiliated clinics.</td>
<td>-3</td>
</tr>
<tr>
<td>A complex organizational/governance structure.</td>
<td>-3</td>
</tr>
<tr>
<td>New/revised policies and procedures can inconvenience workforce members.</td>
<td>-3</td>
</tr>
<tr>
<td>Difficult to choose outside consultants.</td>
<td>-4</td>
</tr>
</tbody>
</table>

Table 4. Factor 1: Socially motivated CIOs.

<table>
<thead>
<tr>
<th>Characterizing Statements</th>
<th>Scores</th>
</tr>
</thead>
<tbody>
<tr>
<td>Significant Barriers</td>
<td></td>
</tr>
<tr>
<td>Inadequate staff to implement changes.</td>
<td>4</td>
</tr>
<tr>
<td>Inadequate funds/budget for implementing changes.</td>
<td>3</td>
</tr>
<tr>
<td>Insufficient time to implement changes.</td>
<td>3</td>
</tr>
<tr>
<td>Inappropriate employee access authorization.</td>
<td>2</td>
</tr>
<tr>
<td>Lack of potent password management policies/procedures.</td>
<td>2</td>
</tr>
<tr>
<td>Outdated information technology.</td>
<td>2</td>
</tr>
<tr>
<td>Neutral</td>
<td></td>
</tr>
<tr>
<td>Education and training of workforce members.</td>
<td>0</td>
</tr>
<tr>
<td>Clinicians can copy PHI and paste to their own files.</td>
<td>0</td>
</tr>
<tr>
<td>Some LANs are outside the control of the hospital’s IT department.</td>
<td>0</td>
</tr>
<tr>
<td>Handheld devices can cause security problems.</td>
<td>0</td>
</tr>
<tr>
<td>Loading of local applications to store or process PHI.</td>
<td>0</td>
</tr>
<tr>
<td>Co-existing manual and electronic patient medical records.</td>
<td>0</td>
</tr>
<tr>
<td>Insignificant Barriers</td>
<td></td>
</tr>
<tr>
<td>Change itself is difficult.</td>
<td>-2</td>
</tr>
<tr>
<td>Workforce members must relearn work procedures.</td>
<td>-2</td>
</tr>
<tr>
<td>Insufficient policies/procedures regarding system access by non-employees, i.e., physicians of affiliated clinics.</td>
<td>-2</td>
</tr>
<tr>
<td>New/revised policies and procedures can inconvenience workforce members.</td>
<td>-3</td>
</tr>
<tr>
<td>The organizational culture will be resistant to it.</td>
<td>-3</td>
</tr>
<tr>
<td>A complex organizational/governance structure.</td>
<td>-4</td>
</tr>
</tbody>
</table>

Table 5. Factor 2: Resources motivated CIOs.
and outdated information technology (statement 17, 0).

In summary, members sorted into this factor believe it is the people themselves who created the most significant barriers. They did not believe that funds, budgets, or outdated information technology were big issues; they were not concerned about outside consultants or vendors; and they did not believe a complex organizational structure was a significant barrier.

**Resources Motivated CIOs**

This viewpoint, as shown in Table 5, emphasized an overall lack of tangible resources as the most significant obstacle. Inadequate staff (statement 7, +4), insufficient time (statement 8, +3), and inadequate funds/budget (statement 4, +3) were sorted as the most significant barriers. A higher score was given to statement 3 (inadequate executive leadership/supervisors) than other groups.

At the same time, these CIOs reported that they believed that they had a great deal of work to accomplish to comply with the law. They believed that there were insufficient or inappropriate policies and procedures: inappropriate employee access authorization (statement 11, +2) and a lack of potent password management policies and procedures (statement 13, +2). They were also concerned with outdated information technology (statement 17, +2), which may mean budgets need to be expanded. They gave a higher score to statement 15 (difficult to choose outside consultants). These CIOs may consider it costly to hire outside consultants, or they may not have the resources to meet the consultants’ recommendations.

For this group, organizational culture or structure was not a significant barrier (statement 6, -4; statement 5, -3). These CIOs did not think change was difficult (statement 1, -2); they did not believe it would be difficult for workforce members to relearn work procedures (statement 9, -2), and they did not believe that new or revised policies and procedures would inconvenience workforce members (statement 10, -3).

All the neutral statements for this group were human behavioral barriers: education and training of workforce members (statement 16, 0); clinicians can copy PHI and paste to their own files (statement 20, 0); some LANs are outside the control of the hospital’s IT department (statement 21, 0); handheld devices can cause security problems (statement 22, 0); loading of local applications to store or process PHI (statement 23, 0); and co-existing manual and electronic patient medical records (statement 25, 0).

Taken together, this factor believed that a lack of tangible resources is the most significant barrier. With enough funds or a bigger budget, some of these barriers could disappear, they believe.

**Discussion**

As a member of the senior management team, the CIO in the healthcare organization plays an important role in strategic planning and practical measures for implementing HIPAA. The sorting results showed different views that can help healthcare organizations to identify a variety of opinions about possible implementation barriers. In addition, the statement profile of each factor suggested the possibility of common challenges to the implementation of the HIPAA security rules in subjects’ organizations, as well as showing the subjective attitudes of the CIOs.

**Socially motivated CIOs.** The significant barriers that socially motivated CIOs focused on are not easily corrected human factors, but they can be reduced with appropriate measures. As with any other project, the success of a security rule implementation is ultimately determined by the acceptance of workforce members. There are many examples that show the importance of user involvement. CEDARS-SINAI Medical Center, the largest private hospital in the western U.S., suspended a computerized provider order entry system last January after 400 physicians complained that it was difficult, time-consuming, and posed risks to patient safety. The hospital’s decision was extraordinary, but not unique. The Cedars-Sinai case reinforces the importance of people issues in successful implementations.

The implementation of HIPAA’s security rule brings significant changes to healthcare organizations, and it has an impact that is neither easily planned nor ostensible. New policies and procedures must be developed, new committees established, and new personnel hired. Those who are knowledgeable about HIPAA are empowered, while others may feel confused. Appropriate management of organizational effects at all levels is essential for successful implementation.

Staff members should be the most valued resources of healthcare organizations. Only those healthcare organizations that can effectively manage their human resources can survive in this highly competitive environment. In organizations in which the employees feel empowered and involved, there is a sense of excitement about helping to make the organization better. In Cedars-Sinai’s case, the hospital believed that by working with a 40-physician medical executive committee, it had sufficiently involved physicians in the design and implementation process. However, rank-and-file physicians believed that the committee did not represent their interests.

The implementation task force for the security rule should work as a bridge, and all the workforce members
should be actively involved in the implementation process. In the task force, there should be representatives from all departments that are covered by the rule. The representatives should be willing to assimilate HIPAA requirements, clearly communicate the mandated conditions to associated personnel and enlist the cooperation of all necessary personnel. Healthcare organizations need to make sure employees have reasonable control of their own operating procedures and guidelines; employees also should have direct influence on the decisions affecting their work. 

Early training will help involve workforce members. The need for the implementation of the security rule must be clearly communicated. Impetus, purpose, content, and scope of the proposed change should be explained to people. Employees need to know the definition of the HIPAA security rule; why it is necessary; who will benefit and how; who will be significantly involved; and what procedures will be introduced. 

Just relaying information about the rule is not enough to create a successful implementation—change management is critical. It is crucial to set reasonable goals and manage expectations. For a huge project like HIPAA, staged training is needed. After the initial introductory training, employees should be continuously notified of the progress of the implementation. For busy clinicians and staff, lengthy training is neither possible nor necessary; the training materials should reflect this.

**Resources-Motivated CIOs.** These CIOs believed that they were short of resources to implement the rule. There was some (+1) concern about statement 7: inadequate executive leadership/supervisors. The first step may be to enlist help from executive leaders to support the importance of HIPAA compliance. The support from executive leaders could mean more budget and personnel allocation. It is difficult to measure the benefits of the security rule implementation in terms of return on investment (ROI), which frequently is used as the only criterion for decision-making. Unfortunately, ROI does have practical shortcomings. According to Bauer, one of the ROI’s most serious problems is absence of consistency. It also has other problems, like the imprecise numeric values for variables and the inherent subjectivity of ROI analysis. 

ROI calculation should be driven more by the values and strategic direction of organizations. Besides quantifiable financial benefits, other potential returns should be included. The implementation of the security rule could bring intangible benefits to healthcare organizations, such as quality improvement, patient satisfaction, cost avoidance, and enhanced hospital reputation. 

HIPAA compliance is attractive to patients, who are increasingly concerned about the privacy and security of health information, which is directly related to their personal and social lives. With the implementation of the security rule, not only the confidentiality of personal information is protected, but also the integrity and availability of EPHI, essential for high-quality healthcare. Quality of service is one of the major reasons why patients select one hospital over another. 

Through the implementation of the security rule, potential threats and vulnerabilities of organizations’ EPHI can be identified. These risks could be mitigated or eliminated by implementing appropriate countermeasures. Inappropriate EPHI disclosure might be prevented, possible lawsuits might be avoided, and patient satisfaction could be elevated. 

The security rule does not require organizations to use sophisticated information technology to secure EPHI. In many cases, the education of employees to conform to changed procedures or processes will be sufficient. These two factors, socially motivated CIOs and resources-motivated CIOs, have distinct views regarding the implementation barriers of the security rule. One group is concerned about barriers related to human behavior; the other believes that the lack of resources is the most important barrier.

Besides the differences, these two groups share some consensus statements. For example, both of them considered the statement “inadequate staff to implement changes” to be a significant barrier. Of course, “inadequate staff” can be interpreted in different ways. It can mean an insufficient number of staff; it can mean non-enthusiastic or non-motivated employees; and it also can mean staff with inadequate skills or training to cope with the implementation of the rules. In fact, people and resource barriers are closely related to each other, and it is not appropriate to deal with them separately. If healthcare organizations can successfully deal with people issues, some resource barriers could go away; for example, when workforce members are fully involved and cooperative, it may need to hire new staff, and the timeframe for the implementation may be shortened.

**Conclusions**

There is no single security rule implementation strategy that works for all covered entities. Multiple barriers need to be identified and managed for successful implementation of the rule. This study is the first that tries to examine issues associated with implementation of the security rule. A qualitative study with a sample of convenience, different types of CIOs’ viewpoints toward barriers to HIPAA imple-
mentation were identified and categorized. The study begins to shed light on the attitudes and perceptions of CIOs as they begin rule implementation. Current CIOs can use this information as a way to begin to examine what the prevailing attitude may be at their institution and, therefore, how to begin building a successful implementation strategy.

Q-methodology is a powerful tool for subjectivity study. It is different from ordinary surveys, which require a big sample size for a valid result. Using Q-methodology, sample sizes are defined statistically in terms of the number of statements to be sorted rather than the number of respondents making the sort. In this study of five participants in the Chicago area, varying viewpoints were extracted. However, to know the distribution of these viewpoints or to expand the results to a bigger area, more participants should be surveyed.

Another important characteristic of Q-methodology is that different people with different backgrounds can be surveyed using the same sample. CIOs' views were examined in this study. In the future, other groups of people can be observed. For example, consultants who have been hired to facilitate the security rule implementation could be surveyed. They may look at these possible barriers from a different aspect; it will be interesting to discover new viewpoints. In the immediate future, however, healthcare administrators should take into consideration the possibility of divergent opinions about barriers to the implementation of the security rule as they plan to meet upcoming deadlines.

**About the Authors**

Mei Ao, MD, MS, is a physician with six years of clinical experience. She had HIPAA privacy rule implementation experience at the University of Illinois at Chicago Medical Center.

Rosemary Walker, DDS, MBA, MS, is a clinical assistant professor and associate program coordinator of health informatics in the Department of Biomedical and Health Information Sciences at the University of Illinois at Chicago.

**Acknowledgment**

We would like to thank Dr. Annette L. Valenta and Dr. Nina M. Olesinski for their help with the Q-sample building and reviews of the drafts. We also would like to thank Dr. Robert G. Mrtek for the help with Q-analysis.

---

**References**


12. Qmethod software is available at http://www.rz.uni-hb-muenchen.de/~p11hs/mqmethod/


Congratulations to the following individuals who have achieved the Certified in Healthcare Privacy (CHP), Certified in Healthcare Security (CHS), and Certified in Healthcare Privacy and Security (CHPS) credentials from July 3 through November 30, 2004. The CHP, CHS, and CHPS credentials recognize those individuals who have met the eligibility requirements and passed the examination. CHP, CHS, and CHPS encourage continued personal and professional growth in the practice of healthcare privacy and security, and provide a national standard of knowledge required for certification. In addition, the credential assists employers, the public, and members of the healthcare profession in the assessment of healthcare privacy and security professionals.

CHP
Anthony P. Amos – Bothell, WA
Bonita N. Boatright – Cortland, OH
Dodie D. Bradshaw – Hummelstown, PA
Dovie H. Brady – Baton Rouge, LA
Rebecca A. Buegel – Casa Grande, AZ
Jane Burster – Tacoma, WA
Rebecca A. Colwell – Forest, VA
Lynn M. Crothers – Lexington, KY
Katherine E. Downing – Nashville, TN
Judith K. Gohman – Cottage Grove, MN
Michael K. Harrington – Thorndale, PA
Crystal Hemmenway – Allen, TX
Patricia E. Henrikson – Phoenix, AZ
Diana L. Henthorne-Stoddard – East Lansing, MI
Cynthia L. Hunter – Boiling Springs, PA
Kimberly A. Jackson – San Diego, CA
Joy M. Jacobsen – Overland Park, KS
Barbara L. Kowalski – Thorndale, PA
Kim C. Kramer – Brandon, MS
Cindy A. Kramer – Boiling Springs, PA
Kim C. Kramer – Pearcy, TX
Shirlee M. Marymee – North Highlands, CA
Patricia A. Murtagh – Torrington, CT
Cindy Nichols – Nashville, TN
Tonya E. Okon – Moreno Valley, CA
Krista D. Rector – Cloverdale, CA
Catherine I. Ronzo – North Las Vegas, NV
Patricia M. Servatius – Utica, NY
Jinger Sherrill – Nashville, TN
Christos Sierros – Miami Beach, FL
Colleen G. Simianer – Scottsbluff, NE
Clarice P. Smith – Hendersonville, NC
Bonnie M. Stejskal – Hudson, WI
Dee F. Vandercook – Nipoma, CA
Sheila G. Walker – Rossey City, TX
Diana M. Warner – Eden Prairie, MN
Lavonne R. Wieland – Apple Valley, MN
Leigh Ann M. Wirh – Nashville, TN
Melissa A. Wiswell – Kyle, TX
Susan L. Woodall – Torrance, WA

CHS
Scott M. Brich – Chesapeake, VA
Thomas R. Walsh – Overland Park, KS

CHPS
Donald P. Brannan – Montgomery, AL
Nadia Fahim-Koster – Duluth, GA
Marie I. Gardenier – Wilmington, DE
Gail A. Kraft – Marietta, GA
Gary R. Sweeney – Littleton, NH
Andrea B. Thomas – Lancaster, PA
Kathy J. Westhafer – West Chester, PA

Join this elite group.
Go to www.himss.org to find out more about the CHP, CHS, and CHPS certification programs.
To see a full listing of certificants go to http://www.himss.org/content/files/chs_certificants.pdf.