Information Management for State Health Officials

HIPAA Privacy Rule Implementation in State Public Health Agencies

Successes, Challenges, and Future Needs

ASSOCIATION OF STATE AND TERRITORIAL HEALTH OFFICIALS

HIPAA Privacy Rule Implementation in State Public Health Agencies — Successes, Challenges, and Future Needs

This project was made possible with funding from the Centers for Disease Control and Prevention, Health Information Privacy Office, Cooperative Agreement to Improve the Nation's Public Health Infrastructure with State Public Health Agencies/Systems (#U50-CCU313903-06). ASTHO is grateful for this support.

The Association of State and Territorial Health Officials is the national non-profit organization representing the state and territorial public health agencies of the United States, the U.S. territories, and the District of Columbia. ASTHO's members, the chief health officials in these jurisdictions, are dedicated to formulating and influencing sound public health policy, and assuring excellence in state-based public health practice.

For additional information contact: publications@astho.org

1275 K Street, NW, Suite 800
Washington, DC 20005
Phone: (202) 371-9090
Fax (202)371-9797
www.ASTHO.org
www.StatePublicHealth.org

Executive Summary

To assist states with implementation of the Health Insurance Portability and Accountability Act (HIPAA), the Association of State and Territorial Health Officials (ASTHO) developed a brief survey to evaluate states' experiences with the Act. The survey was distributed in August 2004 to state senior deputies, members of ASTHO's HIPAA Task Team, and designated state staff members. This issue report presents the survey results, including how states have classified themselves under the Privacy Rule, their outstanding achievements, implementation barriers, and how those barriers have been overcome.

HIPAA, the Federal Privacy Rule, and Public Health—An Overview

Issued under the Health Insurance Portability and Accountability Act of 1996, the federal Privacy Rule provides individuals with new protections regarding the confidentiality of their health information and establishes new protections for health care providers, health plans, and other entities to protect such information.[1] On April 14, 2003, most entities were required to be in compliance with the Privacy Rule.

How State Public Health Agencies Are Classified Under HIPAA

The Privacy Rule classifies entities based on whether an agency includes covered or non-covered functions. These classifications are defined as either a covered entity or a hybrid entity.

- Thirty-two states (64 percent) out of the 50 states surveyed classified themselves as hybrid entities.
- Fourteen states (28 percent) classified themselves as covered entities.
- Four states (8 percent) said they were in the "other" category.

No state reported a change of status during the survey conducted by ASTHO. However, new state legislation could lead to a change in one state's classification.

Achievements

States dedicated considerable effort to train employees on the Privacy Rule and its requirements. Several states highlighted web-based training efforts, monthly newsletters that raise employees' awareness of HIPAA, and individual, face-to-face training efforts. In addition, some states modified their statutes to conform with HIPAA, although the Privacy Rule does not pre-empt state privacy laws that are more stringent or more protective.

Implementation Barriers

The Privacy Rule specifically allows for disclosures of protected health information to public health authorities. However, several states reported a reluctance to comply with this provision, or a general lack of understanding among entities. This lack of understanding was overcome or lessened by training the workforce and educating healthcare providers about the Privacy Rule and how it impacts public health.

Many states commented that they have had limited resources to implement the Privacy Rules. Although this response was a primary answer to our question about barriers to implementation, states also commented they felt they did a good job with the funding and human resources that were available.

Conclusion

States highlighted their achievements in training and education, developing resources for both internal and external use, aligning state laws and regulations to HIPAA, and conducting on-site reviews. As always, there are challenges to any new regulation. The states experienced challenges and responded by providing more knowledge and resources.

About ASTHO

The Association of State and Territorial Health Officials (ASTHO) is the national nonprofit organization representing the state and territorial public health agencies of the United States, the U.S. Territories, and the District of Columbia. ASTHO's members, the chief health officials of these jurisdictions, are dedicated to formulating and influencing sound public health policy and to assuring excellence in state-based public health practice. Guided by its policy committees, ASTHO addresses a variety of key public health issues and publishes newsletters, survey results, resource lists, and policy papers that assist states in developing public policy and promoting public health programs at the state level.

About the HIPAA Task Team

Due to the complexity of the Health Insurance Portability and Accountability Act (HIPAA) rules coupled with the timeframe for implementation, ASTHO formed a group that could identify and share states' needs for HIPAA Privacy Rule implementation. The purpose of the HIPAA Task Team (HTT) is to identify issues that impact primarily state health departments—recognizing many of these same issues will pertain to local health departments. The HTT, which has been in place for more than three years, consists of senior leaders in state health departments as well as members of the National Association of County and City Health Officials (NACCHO), ASTHO affiliate organizations, and other interested organizations. ASTHO has provided leadership by developing forums for states and other interested parties to discuss the HIPAA rules as they pertain to public health.

ASTHO is working with the Centers for Disease Control and Prevention (CDC) Health Information Privacy Office's Privacy Rule Coordinator, Beverly Peeples, JD, and Antonia J. Spadaro, EdD, RN, Acting Privacy Rule Support Officer, to continue the HTT forums and to write issue reports on the topics considered in each forum. The topic for this fifth issue report in the "Information Management for State Health Officials" series is: HIPAA Privacy Rule Implementation in State Public Health Agencies—Successes, Challenges, and Future Needs. It includes a review of outstanding achievements and implementation barriers, and how the barriers have been overcome according to the responses in ASTHO's 2004 survey.

The information in this paper is largely based on the results of the aforementioned survey, in conjunction with follow-up interviews with the following individuals: Mary Beth Joublanc, ADHS HIPAA Compliance Officer and Project Manager, Division of Information Technology Services, Arizona Department of Health Services; Judy Powell, Privacy Officer, HIPAA Program, Arkansas Department of Health; Ed Wilson, Attorney, State of Kentucky; Dave Orren, Data Practices Coordinator, Minnesota Department of Health; Robert Martin, HIPAA Support, North Carolina Division of Public Health; Darlene Bartz, Chief, Health Resource Section, HIPAA Coordinator and Privacy Officer, North Dakota Department of Health; Michael Mullen, Assistant Attorney General, State of North Dakota; Mike Ewald, Director, Records Evaluation and Support Division of Community Health Services, Oklahoma State Department of Health; Elizabeth Potter, Senior Counsel for Administration and HIPAA, Privacy Officer, South Carolina Department of Health and Environmental Control; and Kevin DeWald, HIPAA Compliance Officer, South Dakota Department of Health.

Other reports in this series include:

- *Integrating Child Health Information Systems While Protecting Privacy: A Review of Four State Approaches*
- *Meeting the Challenges Presented by the HIPAA Privacy Rule in Public Health Practice*
- *The Impact of the HIPAA Privacy Rule on Syndromic Surveillance*
- *Data Sharing with Covered Entities Under the HIPAA Privacy Rule: A Review of Three State Public Health Approaches*

These reports are available on the ASTHO website at www.astho.org.

INTRODUCTION

In order to assist states with implementation of the Health Insurance Portability and Accountability Act (HIPAA), the Association of State and Territorial Health Officials (ASTHO) developed a brief survey to evaluate states' experiences with the Act. The survey was distributed in 2004 to state senior deputies[a] and HIPAA Task Team (HTT) members.

The questions asked in the survey and addressed in this paper are:

- How is the public health authority in your state classified according to HIPAA?
- Has your classification (e.g., covered entity, hybrid entity) changed in the past year? If so, please clarify/explain.
- What has your organization done in the implementation of HIPAA that you consider outstanding or that you would like to share with others?
- What are the major barriers that you continue to experience? Please provide examples.
- How might these barriers be overcome?
- On which provisions of HIPAA would you like more guidance?
- Which of the HIPAA Task Team activities has been helpful to you and your staff?

ASTHO received responses from 39 state public health agencies. In order to get a complete national picture, ASTHO contacted the 11 remaining states regarding whether their public health authority classification had changed during the past year.

The results of the survey have been distributed to the HTT for the benefit of shared knowledge through state-to-state experiences and lessons learned. ASTHO has since followed up on priority issues identified from the survey in HTT conference calls. Some priority issues that have been discussed are:

- The Family Educational Rights Privacy Act (FERPA) and its relationship to the Privacy Rule.
- The National Provider Identifier.
- Law Enforcement and the Privacy Rule.
- Protecting Privacy during Large Scale Events.

The HTT continues to address issues raised in the survey. The ASTHO issue briefs and HTT conference calls were selected as the number one and two most helpful HIPAA-related services provided by ASTHO.

This issue paper presents the survey results, including how states have classified themselves under the Privacy Rule, their outstanding achievements, implementation barriers, and how those barriers have been overcome. The information in this paper is largely based on the results of the aforementioned survey, in conjunction with follow-up interviews with selected states whose stories are featured in the following pages.

The Federal Privacy Rule, and Public Health — An Overview

Issued under the Health Insurance Portability and Accountability Act of 1996, the federal Privacy Rule was intended to provide individuals with new protections regarding the confidentiality of their health information and to establish new protections for health care providers, health plans, and other entities to protect such information.[2] On April 14, 2003, most entities were required to be in compliance with the Privacy Rule.

The Privacy Rule addresses the use and disclosure of individuals' health information and establishes an individuals' right to obtain and control access to this information.[3] Specifically, the rule covers "protected health information," defined as individually identifiable health

[a] Because each State Public Health Agency's organizational structure and job titles differ, "Senior Deputy" is a term used by ASTHO to refer to the individuals that typically serve in the second highest leadership position in a State Public Health Agency or to the second highest position itself.

information that is held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.[4] Individuals have the right to:

- Access, inspect, and copy their protected health information and also to request amendments to their records.
- Receive written notice of the uses and disclosures of their health information that may be made by a covered entity, as well as written notice of the individual's rights and the entity's duties with respect to that information.
- Request a listing of disclosures of their protected health information that is shared with others for purposes other than treatment, payment, or health care operations.

In addition, an individual can complain directly to a covered entity or file a complaint with the U.S. Secretary of Health and Human Services regarding non-compliance with the Privacy Rule.

Privacy Rule protections are extended to all individuals, regardless of the state in which they live or work, but the rule does not pre-empt state privacy laws that are more stringent or more protective.[5]

Certain requirements had to be met as of April 14, 2003. In particular, a covered entity was required to:

- **Develop policies and procedures for protecting health information**. These requirements included the maintenance of administrative, technical and physical safeguards, the designation of a privacy official, the mandatory training of employees on the entity's privacy policies and the development of procedures to receive and address complaints.
- **Limit information used and disclosed to the minimum necessary**. Covered entities must make reasonable efforts to limit their employees' access to identifiable health information to the minimum needed to do their jobs.
- **Account for disclosures of protected health information**. Upon request, covered entities must provide individuals with an accounting of disclosures of their protected health information made in the preceding six years. This does not include disclosures for treatment, payment, or operating purposes, including those mandated by law—such as certain disclosures to public health entities and law enforcement agencies.
- **Ensure that "downstream users" protect the privacy of health information by implementing business associate agreements**. Covered entities must enter into a contract or other written agreement with any business associates with whom they share protected health information for various purposes.[6]

A public health authority is defined as: "An agency or authority of the United States, a state, a territory, a political subdivision of a state or territory, or an Indian tribe, or a person or entity acting under a grant of such authority from or contract with such public agency or its contractors or person or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate."[7]

The Privacy Rule was not intended to directly affect the public health community. Public health authorities are not subject to the Privacy Rule when they are conducting public health activities as defined in the Rule, even when they are covered entities acting in the capacity of a public health authority.[8] This is commonly referred to as the public health exception.

The Privacy Rule specifically allows for disclosures to public health authorities without an authorization. Covered entities may disclose protected health information for these public health activities or purposes: to a public health authority authorized by law to collect or receive information for preventing or controlling disease, injury or disability; or for the conduct of public health surveillance, investigations, and interventions.[9]

CLASSIFICATION OF STATE PUBLIC HEALTH AUTHORITIES UNDER HIPAA

The Privacy Rule classifies entities based on whether an agency includes covered or non-covered functions. These classifications are defined as either a covered entity or a hybrid entity. The decision to classify a state a certain way takes a thorough analysis of the functions taken on by the health department and their divisions.

Most of the states that responded to the survey declared themselves hybrid entities (See chart below). In fact 32 states (64 percent) out of the 50 state public health agencies surveyed said their state health agency is a hybrid entity.

Covered vs. Hybrid Entities

A covered entity is a "health plan, health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a transaction."[10]

A hybrid entity is "a single legal entity that is a covered entity, whose business activities include both covered and non-covered functions, and that designates health care components" in accordance with the Privacy Rule.[11]

Fourteen states (28 percent) classified their state public health agency as a covered entity, and four states (8 percent) said they were in the "other" category. States that classified themselves as "other" in our survey were neither a covered entity, nor a hybrid entity.

State Privacy Rule Classification as of 2004

State	HIPAA Status		State	HIPAA Status
Alabama	Hybrid		Montana	Covered
Alaska	Covered		Nebraska	Covered
Arizona	Hybrid		Nevada	Hybrid
Arkansas	Covered		New Hampshire	Covered
California	Covered		New Jersey	Hybrid
Colorado	Other		New Mexico	Covered
Connecticut	Hybrid		New York	Hybrid
Delaware	Hybrid		North Carolina	Hybrid
Florida	Hybrid		North Dakota	Hybrid
Georgia	Covered		Ohio	Hybrid
Hawaii	Hybrid		Oklahoma	Covered
Idaho	Hybrid		Oregon	Covered
Illinois	Hybrid		Pennsylvania	Hybrid
Indiana	Hybrid		Rhode Island	Hybrid
Iowa	Other		South Carolina	Hybrid
Kansas	Hybrid		South Dakota	Hybrid
Kentucky	Hybrid		Tennessee	Covered
Louisiana	Covered		Texas	Hybrid
Maine	Other		Utah	Hybrid
Maryland	Hybrid		Vermont	Hybrid
Massachusetts	Hybrid		Virginia	Hybrid
Michigan	Hybrid		Washington	Hybrid
Minnesota	Other		Wisconsin	Hybrid
Mississippi	Covered		West Virginia	Hybrid
Missouri	Hybrid		Wyoming	Covered

The overwhelming percentage of states classified as hybrid entities has left some states curious as to whether they should change their classification from covered entity to hybrid entity. The survey showed that no state reported they had changed classification since their initial declaration under the Privacy Rule. Currently, a small number of covered entities are in the research phase to determine the feasibility of a status change.

In Arkansas, the Department of Health (DOH) carefully weighed the options in choosing a classification. At first glance, the hybrid entity seemed to fit their organizational structure. Arkansas realized, however, that protected health information could be found throughout the agency, especially since they are housed with providers, and that all their employees required general HIPAA training, at a minimum. The Arkansas DOH also realized the public health reporting aspect would be easier if it took a covered entity status. For instance, if a large-scale disaster occurred and Arkansas DOH was a covered entity, it could notify the press immediately if there was a serious threat to public health. The DOH director or designee would make that decision based on established standards of public health practice.

New state legislation[12] on August 11, 2005, made the Arkansas DOH a division of the Arkansas Department of Health and Human Services. This reorganization could possibly change the DOH's covered entity classification. The Department of Health and Human Services as a whole may not be required to keep that classification if only certain portions of the department as a whole perform functions that would be covered by HIPAA.

ACHIEVEMENTS

A. Employee Training and On-Site Reviews

Responding states indicated that considerable effort was dedicated to training employees on the Privacy Rule and its requirements. Several states highlighted web-based training efforts, monthly newsletters that raise employees' awareness of HIPAA, and individual, face-to-face training efforts. Below are examples of state public health agency achievements.

Arkansas

The Arkansas Department of Health, a covered entity at the time of this discussion, implemented Web-based training for the entire workforce, approximately 2,800 employees, allowing colleagues as well as contractors the opportunity to receive HIPAA training. In addition, a member of the legal team and the HIPAA Privacy Officer traveled around the state conducting seminars for colleagues. These training sessions were held at local health department staff meetings. The traveling team quickly noticed that the face-to-face meetings were helpful not only to those being trained, but for the development of future policies and procedures as well. The question and answer portion presented situations that were new to both sides. Follow-up training is conducted at the rate of approximately 20 employee work units per year.

Minnesota

The Minnesota Department of Health (DOH), which classified itself as "other," collaborated with other state agency leaders to organize HIPAA education for Minnesota state agencies. The HIPAA Review Board was a group of state agencies that collaborated on the analysis and implementation of HIPAA for state government agencies. The following agencies participated in the HIPAA Review Board:

- Administration (information policy analysis division)
- Attorney general's office
- Children, families, and learning
- Corrections
- Emergency medical services regulatory board
- Employee relations
- Health
- Human services
- Information policy council
- Labor and industry
- Minnesota state colleges and universities
- Office of technology
- Public safety.

The HIPAA Review Board developed a HIPAA assessment specific to Minnesota state agencies. The governor's office distributed the assessment to more than 120 state agencies, boards and commissions. The departments of health, human services, and administration delivered a basic HIPAA training on how to complete the assessment on August 29, 2002, to 45 people from 31 state agencies, boards, and commissions. About 35 assessments were returned. Minnesota DOH reviewed the assessments for common issues and contacted any agencies that had questions.

The HIPAA Review Board delivered two training sessions: the basic HIPAA training described above, and a HIPAA Continuing Legal Education seminar for government attorneys. Minnesota DOH did the HIPAA Continuing Legal Education seminar in conjunction with the Minnesota County Attorneys Association on January 10, 2003. About 125 persons from state agencies, cities, counties, the Office of the Attorney General, Minnesota state colleges and universities, and the state legislature attended this full-day training.

North Dakota

While drafting Privacy Rule policies and procedures, the North Dakota Department of Health, a hybrid entity, also included HIPAA Security Rule policies and procedures. This combination allowed employees to receive all the training at once, instead of undergoing

individual training on privacy followed by security training later in the year. Updates on policies and procedures are communicated in an annual staff training exercise.

Oklahoma

The Oklahoma State Department of Health, a covered entity, provided HIPAA training on a large scale to over 2400 employees prior to May 2003. The training was targeted to three different groups in the following manner:

Group 1 consisted of direct providers at the county health department level. The health department conducted a series of nine telecommunication presentations with question and answer sessions that gave specific information needed for front line provider staff. This group included clerks, environmental health practitioners, medical staff, and nurses. Total staff trained in this group was approximately 1,300.

Group 2 consisted of central office staff who did not normally come in contact with protected health information or clients. The health department provided a web-based training that gave general information about the privacy rule. The Web site tracked each enrolled employee's progress and issued a certificate upon completion of the training. Total staff trained in this group was approximately 600.

Group 3 consisted of central office staff whose jobs require access to protected health information. This group consisted primarily of staff involved in public health surveillance and regulatory activities, and included directors, chiefs, long-term care staff, information technology staff, and jail inspectors. The trainings consisted of group meetings in which each employee was trained and had the opportunity to ask questions. The total number of staff trained in this group was approximately 300-400.

Follow-up training was conducted for the employees in the first group in October 2004. The coordination of training for new employees is the responsibility of each supervisor.

South Carolina

The South Carolina Department of Health and Environmental Control (DHEC), a hybrid entity, has a HIPAA Oversight Committee that includes four smaller subcommittees. In 2004, the Compliance Subcommittee developed a compliance assessment tool to monitor and evaluate the success of the agency's implementation of HIPAA privacy and security requirements. The agency had previously conducted an annual physical security survey of each area that handled protected health information. This survey form was expanded into a HIPAA Assessment Checklist that measures compliance with, among other items:

- Physical security of protected health information including electronic information.
- Completion and proper documentation of workforce HIPAA training (employees, volunteers, students/interns, etc.)
- Compliance with HIPAA policies and procedures in clinic operations (e.g., proper use and documentation in the medical record of disclosures pursuant to HIPAA-compliant authorizations, proper use and filing of the Notice of Privacy Practices Acknowledgement Form, etc.)

Prior to April 14, 2003, the HIPAA Privacy Rule enforcement date, the South Carolina DHEC developed an in-house training program that included three levels of staff training depending on the amount of access an employee had to protected health information. The training was delivered by a combination of video and live presentations.

Level One: South Carolina's HIPAA 101 is a 53-minute video that provided instruction and training primarily on the HIPAA Privacy Rule. The South Carolina DHEC is a hybrid entity under HIPAA since the agency is South Carolina's public health authority and environmental protection agency, and provides certain health care services through operation of county health departments and home health services. Due to overlapping staff responsibilities, as well as the concern that all

employees safeguard client privacy, South Carolina's HIPAA Training Policy requires all members of its workforce to view the HIPAA 101 training video.

In 2004, the HIPAA Oversight Committee Training Subcommittee began revising the agency's HIPAA 101 privacy training. With the deadline for Security Rule compliance just around the corner, the agency decided to incorporate the required Security Rule training. The revised HIPAA 101 training is a 23 minute video/CD that provides training on both the HIPAA Privacy and Security Rules. All members of the South Carolina DHEC workforce, including approximately 5,000 employees, volunteers, interns and some contractors who work directly with SCDHEC healthcare clients or client protected health information, were required to view the new HIPAA 101 training video by April 2005. Employees beginning employment after April 2005 will also be requested to review the training video.

Levels Two, Three: South Carolina's Advanced HIPAA Training The two levels of expanded HIPAA training are provided to SCDHEC staff working in the covered entity portions of the agency as health care providers and supervisors. These employees receive more detailed information on HIPAA policies and procedures as implemented in the covered entity portions of the agency. The Training Subcommittee has begun work to revise these advanced HIPAA trainings. The revised trainings will include information on specific issues that routinely arise in clinic operations and have formerly been dealt with on a case-by-case basis. Examples include requests for information from the state Department of Social Services, requests for disclosure of health information based upon powers of attorney, child abuse and neglect reporting, and disclosures to law enforcement.

South Carolina's Policies & Procedures Revisions In addition to implementing Security Rule policies and procedures, the HIPAA Oversight Committee Policy Subcommittee recently reviewed existing HIPAA Privacy policies and procedures. Based upon SCDHEC's experience in implementing the HIPAA Privacy Rule over the past two years, five HIPAA policies were revised to provide clarification, reflect changes in agency personnel or program structure, and to improve agency procedures in dealing with certain aspects of HIPAA implementation.

South Dakota

South Dakota's HIPAA Compliance Officer began providing onsite HIPAA compliance reviews to all field offices in September 2003. As of June 2005, half of the 86 field offices within the state have been reviewed. The face-to-face assistance from the South Dakota Department of Health, a hybrid entity, helped relations between the state and field offices. By making the personal connection, the field offices have taken a proactive role with HIPAA compliance.

During the two to four hour visits, the HCO receives a tour of the facility and reviews a compliance check list. The list is made up of security questions regarding protected health information (written, oral, and electronic), accessibility of administrative policies and procedures (in electronic and hard copy formats), and general questions about HIPAA privacy, education, and security. After the tour and review, new staff receive the chance to be trained personally by the state compliance officer. If there are no new employees, an update is given to the entire field office. The South Dakota Department of Health is comprised of seven regions that convene twice a year for an all-staff meeting. This provides another opportunity for the HIPAA compliance officer to administer face-to-face training.

B. Amendment of State Legislation

The Privacy Rule does not pre-empt state privacy laws that are more stringent or more protective.[13] The following states implemented legislative amendments or pre-emption analysis that they felt were beneficial.

Minnesota

The Minnesota Department of Health's HIPAA Review Board members completed a very detailed matrix comparing the HIPAA privacy requirements to:

- Minnesota Statutes, chapter 13, (the data practices act).
- Minnesota Rules, chapter 1205, (data practices act rules).
- Minnesota Statutes, sections 144.335 and 144.651, (the health records act and the Minnesota patient bill of rights).

This 45-page matrix is available on the Minnesota Department of Health's Web site. It has been helpful for comparison purposes of the federal versus state differences.

North Carolina

The North Carolina Division of Public Health (DPH), a hybrid entity, educated its staff on HIPAA confidentiality requirements and how HIPAA interacts with North Carolina General Statutes. This multi-step process began with a workgroup from the North Carolina Health Care Information and Communications Alliance, Inc. (NCHICA),[b] who undertook a preliminary pre-emption analysis comparing state statutes with the specific HIPAA Privacy Rule provisions. After that first review, a more conclusive review was completed with the Chief of Legal and Regulatory Affairs at the Division of Public Health and public health law attorneys from the University of North Carolina - Chapel Hill, Institute of Government.

After the initial pre-emption analysis, further review by the North Carolina Attorney General's Office determined that the North Carolina General Statutes would pre-empt HIPAA in many areas. The core state public health statutes provide more stringent privacy protections than required by HIPAA and would therefore not be pre-empted by HIPAA. Further, the review of applicable North Carolina statutes and Administrative Code confirmed that most public health activities were firmly established in North Carolina law. North Carolina laws conformed to the HIPAA public health carve-out: "[N]othing in this part shall be construed to invalidate or limit the authority, power, or procedures established under any law providing for the reporting of disease or injury, child abuse, birth or death, public health surveillance, or public health investigation or intervention."[14] HIPAA did not pre-empt existing North Carolina public health law.

Particular uses and disclosures are continually reviewed against HIPAA standards and state law to determine whether they are required by North Carolina law or whether disclosures are permitted under the Privacy Rule for public health activities.

This analysis helped the North Carolina DPH focus its training efforts on educating employees about the interrelationship between HIPAA and North Carolina state statutes.

North Dakota

North Dakota's Office of Attorney General reviewed the North Dakota Century Code for all references to confidential health information. Those terms were targeted for modification or substitution to make the state law more consistent with the federal regulations. This legislation substantially reduced the necessity of checking back and forth between state law and HIPAA. Aside from a few exceptions, if one is in compliance with HIPAA, it is safe to assume one is also in compliance with North Dakota state law.

This activity was no easy task. Approximately 30 code sections were changed, either significantly or slightly, to match HIPAA terminology. The reviewers were very careful to use such terms as "authorization," "protected health information," and "disclose/disclosure" in

[b] NCHICA is a nonprofit consortium of over 240 organizations dedicated to improving healthcare by accelerating the adoption of information technology. The Institute of Government supports local and state government issues, including legal guidance.[b]

the manner the terms were referenced in HIPAA.

North Dakota's HIPAA Coalition sought to be more consistent when it came to terminology and HIPAA implementation according to the state law and federal regulations within each organization. The HIPAA Coalition consisted of:

- The North Dakota Department of Human Services
- The Department of Health
- Approximately 28 local public health authorities
- The North Dakota Public Employees Retirement System Health Plan
- The North Dakota Healthcare (Hospital) Association
- The North Dakota Medical Association
- The North Dakota Pharmaceuticals Association
- Many private health care providers.

IMPLEMENTATION BARRIERS

The Privacy Rule was not intended to directly affect the public health community. Public health authorities are not subject to the Privacy Rule when they are conducting public health activities as defined in the Rule, even when they are covered entities acting in the capacity of a public health authority.[15] This is commonly referred to as the "public health exception".

Respondents found the lack of understanding of the public health exception in the Privacy Rule as well as limited funding to be the major barriers during the first year of implementation. Many states overcame these barriers by consulting online resources from the U.S. Department of Health and Human Services, the U.S. Office of Civil Rights, and the Centers for Disease Control and Prevention.

A. Understanding the Public Health Exception

The Privacy Rule specifically allows for disclosures to public health authorities for the following reasons without an authorization:

> For the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions.[16]

Several states reported a reluctance to comply with this provision, or a general lack of understanding among entities regarding how the exception applies to their daily business activities. This lack of understanding was overcome or lessened by training the workforce and educating healthcare providers, etc. about the Privacy Rule and how it impacts public health. The following examples demonstrate how some states have developed helpful resources for their staff and providers to overcome the misunderstandings that occur with the public health exception.

Arizona

The Arizona Department of Health Services (DHS) is a hybrid entity. Its HIPAA Compliance Team developed a verification packet for the Department's programs that access or receive protected health information from covered entities. The documents in the packet verify for covered entities that the Arizona DHS has the authority to access information to meet the department's mission as a public health authority. The HIPAA Team also developed a verification letter specific to the Arizona DHS mission as a health oversight agency; however, this tool is rarely needed. The verification tools help covered entities comply with the Privacy Rule's minimum necessary standard.

The public health authority packet contains a general letter about the authority of the Arizona DHS and an attachment that covers the entire list of programs in the department's Division of Public Health Services. The programs in this division perform the majority of public health authority activities for the department. Another letter was developed for specific public health programs that encounter continued resistance. The packet is currently being updated to reflect new rules, regulations, and legislation.

Mary Beth Joublanc, HIPAA Compliance Officer and Project Manager said, "This packet has helped increase the comfort level of covered entities when public health related information is sent to the department. In the beginning most covered entities were cautious about reporting information. Clarification from the department eased their concerns."

Kentucky

To assist with HIPAA education, the Kentucky Department of Health, a hybrid entity, is planning to bring together public health, private providers, hospitals, ambulance, emergency and law enforcement, and fire organizations. Topics addressed may include the Privacy Rule in a declared or suspected public health event and HIPAA education.

Minnesota

The Minnesota Department of Health, which classified itself as "other," developed information sheets for use by staff members who have contact with covered entities and are reluctant to disclose data to public health agencies because of concerns that HIPAA prohibited the disclosure. The goal was to have each covered entity's attorney review the information sheet, to familiarize the attorneys with HIPAA. The information sheets are very specific and include citations to relevant state and federal law so that attorneys can confidently advise their clients that HIPAA permits disclosing protected health information to public health agencies.

The information sheets also have an analysis of HIPAA disclosure tracking requirements, especially as those related to multiple disclosures of protected health information to the same entity for a single purpose. This analysis was included because some covered entities were reluctant to voluntarily disclose protected health information to public health authorities. The covered entities perceived that HIPAA required the very burdensome tracking of disclosures on an individual basis. Information is included to show that a general log of disclosures could be kept internally, which staff can use to adequately notify patients that their information would be shared with the Department of Health in these certain situations.

North Carolina

HIPAA had a limited impact on data sharing with and within the North Carolina Division of Public Health (DPH), a hybrid entity, because:

- Where the state statutes were stricter than HIPAA, DPH continued to follow the more stringent requirements.
- State statutes requiring public health reporting were not pre-empted.
- Other public health reporting not explicitly required by statute is permitted by the Privacy Rule.

In addition, the definitional clarification of the term "health plan" also worked in North Carolina's favor. The clarification states that government funded programs are not considered health plans. Therefore the government funded public health program was not required to have a covered entity status. This classification was important. It meant while North Carolina DPH as a whole could be a hybrid entity, the primary purpose of which is not to provide healthcare, it has components that perform covered functions. The only component within the North Carolina DPH to qualify as a covered entity is the state laboratory.

In 2004, the North Carolina General Statute 130A-12 was revised to align with the Privacy Rule. This meant that neither the DPH nor local health departments would be required to obtain patient consent to use or disclose individually identifiable health information for treatment, payment, or health care operations purposes, except in limited circumstances required under North Carolina law or by other federal laws. This modification aligned the confidentiality requirements for public health identifying information with the HIPAA standards for treatment, payment, and healthcare operations. As a result, the North Carolina DPH could release, without consent, identifying information for treatment, payment, and healthcare operation purposes consistent with the Final Privacy Rule.

While North Carolina public health law and the Privacy Rule require or permit sharing of data with public health, not all covered entities were attuned to HIPAA exemptions, exceptions, and permitted disclosures. To overcome resistance by covered entities, including sister agencies at the North Carolina Department of Health and Human Services, the DPH developed general and program specific communications describing the Privacy Rule's applicability to public health.

Within the North Carolina DPH, all staff have been trained on HIPAA and the division's status as a hybrid entity. Public health program managers and their staff continue to be trained in the specifics of North Carolina public health laws that staff applies to its programs. Every

manager has an official copy of all applicable North Carolina public health laws (hardcopy and searchable CD-ROM). The North Carolina Office of Legal and Regulatory Affairs and the University of North Carolina Institute of Government provided formal training in public health regulations and continues to provide as-required support and guidance regarding specific regulations. The HIPAA office of the North Carolina DPH continues to work with program management to clarify the interactions between HIPAA and programmatic requirements.

North Dakota

In April 2003 the North Dakota Department of Health, a hybrid entity, drafted a letter to assist efforts to obtain information for public health purposes. This letter addressed concerns about the release of protected health information for the purpose of public health activities. It stated that an authorization is not needed prior to releasing protected health information to a public health authority for public health purposes. It also stated that the organization does not need to execute a business associate agreement with the public health authority prior to releasing the information. The letter listed the privacy officer's name and phone number, in case further clarification was needed.

South Carolina

The South Carolina Department of Health and Environmental Control, a hybrid entity, developed informational materials on public health activities designed to assist other healthcare providers and facilities in under-standing the HIPAA Privacy Rule. The materials also describe state statutes as they relate to disclosures for public health purposes such as disease reporting, surveillance, and public health investigations.

South Dakota

Initially, clinics and hospitals were hesitant to share data with the South Dakota Department of Health (DOH), a hybrid entity, in spite of state laws requiring them to do so. In response, the DOH created a letter to concerned individuals that outlined the public health exception and the ability to share protected health information with a public health authority performing public health activities. South Dakota has not had any problems with providers on this issue.

B. Funding

Many states commented that they have had limited resources to implement the Privacy Rules. Although this was a frequent answer to ASTHO's survey question about barriers to implementation, states also commented they felt they did a good job with the funding and human resources that were available.

States commented that there was no ongoing funding for security audits or Privacy Rule implementation. Because there was no uniform interpretation among partners, confusion exists about which approach is most appropriate. One respondent suggested that state legislatures could allocate more money as an option to solve funding issues. Another respondent commented that the DHHS could relieve the states of certain administrative burdens as a way to alleviate the pressure on funding.

Conclusion

This report explores the results of ASTHO's survey on HIPAA Privacy Rule implementation experiences. Many states have highlighted their achievements in training, developing resources for both internal and external use, aligning state laws and regulations to HIPAA, and performing on-site reviews.

As always, there are challenges to the new regulations imposed by the Privacy Rule. States are experiencing challenges associated with the initial implementation, including the lack of understanding of the public health exception and how that exception is designed to assist state public health authorities. States are responding to this lack of understanding by providing more knowledge and resources. Future state needs include funding for training exercises when updated information is released and resources to upgrade state security components.

ASTHO will continue to feature items of interest gleaned from this survey on HIPAA Task Team conference calls. The next series of conference calls to take place in the fall of 2005 will discuss privacy implications for law enforcement.

Acknowledgements

ASTHO wishes to express its sincere appreciation to the individuals who shared their experiences and provided valuable information, insights, and recommendations for this report. Thank you also to the individuals who provided their invaluable expertise concerning the rules and regulations of the HIPAA Privacy Rule.

Beverly Peeples, JD
Privacy Rule Coordinator
Health Information Privacy Office
Centers for Disease Control and Prevention

Antonia J. Spadaro, EdD, RN
Acting Privacy Rule Support Officer
Health Information Privacy Office
Centers for Disease Control and Prevention

Mary Beth Joublanc, ADHS HIPAA Compliance Officer and Project Manager, Division of Information Technology Services, Arizona Department of Health Services, Personal Communication May 18, 2005

Judy Powell, Privacy Officer, HIPAA Program Arkansas Department of Health, Personal Communication May 18, 2005

Ed Wilson, Attorney, Kentucky, Personal Communication May 18, 2005

Dave Orren, Data Practices Coordinator, Minnesota Department of Health, Personal Communication May 18, 2005

Robert Martin, HIPAA Support, North Carolina Division of Public Health, Personal Communication May 17, 2005

Darlene Bartz, Chief, Health Resource Section, HIPAA Coordinator and Privacy Officer, North Dakota Department of Health, Personal Communication May 16, 2005

Michael Mullen, Assistant Attorney General, North Dakota, Personal Communication May 16, 2005

Mike Ewald, Director, Records Evaluation and Support Division of Community Health Services, Oklahoma State Department of Health Personal Communication May 18, 2005

Elizabeth Potter, Senior Counsel for Administration and HIPAA Privacy Officer, South Carolina Department of Health and Environmental Control, Personal Communication May 19 2005
Kevin DeWald, HIPAA Compliance Officer, South Dakota Department of Health, Personal Communication May 18, 2005

References

Office for Civil Rights. Department of Health and Human Services. Title 45 of the Code of Federal Regulations, Part 160 and 164. http://www.dhhs.gov/ocr/combinedregtext.pdf

Office for Civil Rights. OCR Guidance explaining significant aspects of the Privacy Rule, 2002. Department of Health and Human Services. http://www.hhs.gov/ocr/hipaa

Health Information, First-Year Experiences Under the Federal Privacy Rule, GAO Report to the Chairman, Committee on Health, Education, Labor, and Pensions, U.S. Senate, September 2004.
http://www.gao.gov/new.items/d04965.pdf

Information Management for State Health Officials: Meeting the Challenges Presented by the HIPAA Privacy Rule in Public Health Practice, Association of State and Territorial Health Officials (ASTHO), 2004.
http://www.astho.org/pubs/29725_ASTHO.pdf

HIPAA Privacy Rule and Public Health Guidance from DCD and the U.S. Department of Health and Human Services, 2003.
www.cdc.gov/mmwr/PDF/wk/mm52SU01.pdf

Online Resources

Federal Government Resources

Centers for Disease Control and Prevention Guidelines www.cdc.gov/privacyrule

Centers for Disease Control and Prevention—Division of Public Health Surveillance and Informatics www.cdc.gov/epo/dphsi/index.htm

Department of Health and Human Services Office of Civil Rights—HIPAA Guidelines www.hhs.gov/ocr/hipaa

National Center for Health Statistics www.cdc.gov/nchs/default.htm

National Committee on Vital and Health Statistics www.ncvhs.hhs.gov

National Institutes of Health http://privacyruleandresearch.nih.gov

State Government Resources

Arizona Department of Health Services www.azdhs.gov

Arkansas Department of Health www.healthyarkansas.com

Kentucky Cabinet for Health and Family Services http://chfs.ky.gov

Minnesota Department of Health www.health.state.mn.us

Oklahoma State Department of Health www.health.state.ok.us

North Carolina Department of Health and Human Services www.dhhs.state.nc.us

North Dakota Department of Health www.health.state.nd.us

South Carolina Department of Health and Environmental Control www.scdhec.net

South Dakota Department of Health www.state.sd.us/doh

Associations, Nonprofit Organizations, and Academic Institutions

American Hospital Association—HIPAA www.hospitalconnect.com/aha/key_issues/hipaa

American Medical Association www.ama-assn.org/ama/pub/category/4234.html

Association of State and Territorial Health Officials www.astho.org

Georgetown University Health Privacy Project http://healthprivacy.org

National Association of Health Data Organizations www.nahdo.org

National Governors Association www.nga.org/center/HIPAA

Public Health Grounds HIPAA Privacy Rule: Enhancing or Harming Public Health? www.publichealthgrandrounds.unc.edu/privacy/index.htm

Stanford University Medical School—HIPAA http://hipaa.stanford.edu

Workgroup for Electronic Data Interchange—Strategic National Implementation Process www.wedi.org/snip

---

[1] Pub. L. No. 104-191, §264, 110 Stat. 1936, 2033
[2] Ibid.
[3] 45 CFR §160 and §164
[4] 45 CFR §160.103
[5] Health Information, First-Year Experiences Under the Federal Privacy Rule, GAO Report to the Chairman, Committee on Health, Education, Labor, and Pensions, U.S. Senate, pg 4-6, September 2004
[6] Ibid. pg 6-7
[7] 45 CFR §164.501
[8] 45 CFR §164.512(b)
[9] 45 CFR 164.512(b)(1)(i)
[10] 45 CFR §160.103
[11] §164.105(a)(iii)(c) as defined by the HIPAA Privacy Rule 45 CFR §164.103
[12] House Bill 2341, Act 1954 of the Regular Session 2005
[13] 45 CFR §160.202
[14] Preamble to Final Privacy Rule
[15] 45 CFR §164.512(b)
[16] 45 CFR §164.512(b)(1)(i)

Association of State and
Territorial Health Officials

1275 K Street, NW
Suite 800
Washington, D.C. 20005-4006
www.astho.org