Information Management for State Health Officials

Data Sharing with Covered Entities Under the HIPAA Privacy Rule

A Review of Three State Public Health Approaches

ASSOCIATION OF STATE AND TERRITORIAL HEALTH OFFICIALS

Data Sharing with Covered Entities under the HIPAA Privacy Rule: A Review of Three State Public Health Approaches

This project was made possible with funding from the Centers for Disease Control and Prevention 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

ASSOCIATION OF STATE AND
TERRITORIAL HEALTH OFFICIALS

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

In 1996, the Health Insurance Portability and Accountability Act (HIPAA) was enacted. Among other things, Congress sought to standardize health-care related electronic transactions through HIPAA in recognition that advances in technology could affect the privacy of health information. The resulting HIPAA Privacy Rule was adopted by the U.S. Department of Health and Human Services (DHHS) to address these concerns. The rule went into effect on April 14, 2003.

The Privacy Rule was not intended to directly affect the public health community. The Centers for Disease Control and Prevention (CDC) and other organizations have provided significant guidance on the impact of the Rule on public health practice and research. However, many issues require additional clarification.

This report discusses the differing approaches of three states (Kansas, South Carolina, and Pennsylvania) to sharing protected health information, as well as aggregated data, with covered entities under the HIPAA Privacy Rule. "Covered entity" is defined by the Privacy Rule to include health plans, healthcare clearinghouses, and most healthcare providers. All three states have encountered and overcome challenges resulting from the implementation of the HIPAA Privacy Rule.

In the post-HIPAA environment, the Kansas Department of Health and Environment launched a pilot project to share county-level tuberculosis (TB) data with physicians. This system also allowed all the counties in their state system to access TB data. Such access helped serve populations that routinely move across county borders.

The Pennsylvania Department of Health described its approach to data sharing with covered entities for research and for public health investigation. Pennsylvania has explored approaches to assist covered entities in data sharing to decrease burdens for physicians, hospitals, and clinics that transmit data to public health authorities.

The South Carolina Office of Research and Statistics Budget and Control Board and the South Carolina Department of Health and Environmental Control (DHEC), along with other South Carolina agencies, are working together to develop an integrated data warehouse that will allow for data searches across a number of different information systems. The value of the integrated data system, collection and sharing of data from covered entities, and challenges within the HIPAA Privacy Rule are all discussed.

Key Findings

Key findings or themes resulting from discussions with these states regarding data sharing with covered entities include:

1. While the HIPAA Privacy Rule was not intended to limit information collected for public health purposes, there have been unintended consequences, particularly related to sharing data with covered entities. Many state and local public health departments have spent time and resources educating and working with covered entities to ensure that traditional and new data will be shared with public health departments.

2. Covered entities are an important partner for public health, because they send information critical to public health. Misperceptions and reluctance to continue to send information to public health authorities require greater attention on how to facilitate the flow of information with covered entities.

3. As exemplified by the three different state approaches discussed in this paper, implementation of the HIPAA Privacy Rule and approaches to data sharing vary from state to state. Other federal laws and state laws have been taken into account by the states.

4. Protected health information, information that identifies or provides a reasonable basis to

believe it can be used to identify an individual,[1] is no longer covered under the HIPAA Privacy Rule after it is has been sent to public health authorities. This is not to say the privacy of such data is unprotected. Public health departments adhere to other policies, procedures, and state laws that protect the privacy of individuals. Public health workers understand that protecting the privacy of individuals is critically important and they take this responsibility very seriously.

5. The ability to integrate information across a number of data systems provides public health a number of opportunities to know more about the health of the public and to develop more effective and targeted public health interventions. There is potential for protection of health as well as cost savings as a result. Efforts to integrate systems will always have to be monitored to ensure that privacy issues are considered.

ASTHO has worked with a number of states to explore HIPAA issues and has consistently received feedback that sharing approaches to HIPAA implementation among state public health staff is important. With the assistance of the Centers for Disease Control and Prevention's HIPAA Program Office and other experts such as consultant James G. Hodge Jr., JD, LLM, Executive Director, Center for Law & the Public's Health, Johns Hopkins Bloomberg School of Public Health, we hope to continue to provide states and other partners with the assistance they need to effectively implement the HIPAA rules.

[1] Consistent with section [45 CFR 160.103]

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 ASTHO's policy committees, the organization addresses a variety of key public health issues and publishes newsletters, survey results, resource lists, and policy papers that assist states in the development of public policy and in the promotion of 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 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, 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 (Robin Ikeda, MD, MPH, Associate Director of Science, Epidemiology Program Office, CDC; Beverly Dozier, JD, Privacy Rule Coordinator, CDC; and Linda S. Shelton, Program Administrator) and James G. Hodge Jr., JD, LLM, Executive Director, Center for Law & the Public's Health, Johns Hopkins Bloomberg School of Public Health, to continue the HTT forums and to write issue reports around the topics considered in each forum.

This issue report includes a review of the Privacy Rule's guidelines on data exchange with covered entities, overviews of the presentations made by Kansas, Pennsylvania, and South Carolina from a January 2004 HTT forum teleconference, and key findings.

Introduction

Covered entities, defined by the Privacy Rule to include health plans, healthcare clearinghouses, and most healthcare providers,[2] have traditionally shared surveillance data and protected health information (PHI) with public health authorities. PHI refers to "individually identifiable health information that is transmitted by electronic media, or transmitted or maintained in any other form or medium."[3]

Since April 14, 2003, when the HIPAA Privacy Rule became operational, varying interpretations of the Rule have caused confusion regarding the regulations surrounding data sharing. Many covered entities have refrained from sending appropriate health data to public health authorities because of these uncertainties. Public health authorities, as defined by the Privacy Rule, are agencies acting under a grant of authority that are responsible for public health matters as part of their official mandate.[4]

The Privacy Rule states that a covered entity may disclose protected health information for public health activities and purposes such as preventing or controlling disease, injury, or disability.[5] The Rule permits PHI to be shared for specific public health purposes. The following describes the types of protected health information that can be disclosed by covered

[2] Consistent with section [45 CFR 164.501]
[3] Consistent with section [45 CFR 160.103]
[4] Consistent with section [45 CFR 164.501]
[5] Consistent with section [45 CFR 164.512]

entities for public health purposes without authorization:

Box 1.[6] Protected health information (PHI) disclosures by covered entities for public health activities requiring no authorization under the Privacy Rule

Without individual authorization, a covered entity may disclose PHI to a public health authority that is legally authorized to collect or receive the information for the purposes of preventing or controlling disease, injury, or disability including, but not limited to:

- Reporting of disease, injury, and vital events (e.g., birth or death); and
- Conducting public health surveillance, investigations, and interventions.

PHI may also be disclosed without individual authorization to:

- Report child abuse or neglect to a public health or other government authority legally authorized to receive such reports;
- A person subject to jurisdiction of the Food and Drug Administration (FDA) concerning the quality, safety, or effectiveness of an FDA-related product or activity for which that person has responsibility;
- A person who may have been exposed to a communicable disease or may be at risk for contracting or spreading a disease or condition, when legally authorized to notify the person as necessary to conduct a public health intervention or investigation; and
- An individual's employer, under certain circumstances and conditions, as needed for the employer to meet the requirements of the Occupational Safety and Health Administration, Mine Safety and Health Administration, or a similar state law.

This report, describes three different state approaches and challenges to data sharing with covered entities. Recently, the Kansas Department of Health and Environment (KDHE) and Kansas State University began piloting a program to give one physician's office access to reportable disease information via the HAWK system.[7] KDHE has also implemented an approach whereby all the counties in their state system are able to access TB data in order to serve intrastate, transient populations.

The Pennsylvania Department of Health (PA-DOH) addressed its approach to data sharing with covered entities using two methods: data shared at the research level and data for public health investigation. PA-DOH is also exploring approaches to assist covered entities with data sharing, so that there is decreased burden for physicians, hospitals, and clinics that must send this valuable information to public health authorities.

The Budget and Control Board of the South Carolina Office of Research and Statistics and the South Carolina Department of Health and Environmental Control (DHEC), along with other state agencies, have worked to develop an integrated data warehouse that will allow for data searches across a number of different information systems. The value of the integrated data system, how data from covered entities is collected and shared, and challenges with HIPAA are discussed.

Kansas

System Overview

The HAWK system, similar to the CDC's National Electronic Disease Surveillance System (NEDSS)[8], is a web-based reportable disease surveillance system that enables state and local health departments to collect and analyze information on cases of reportable diseases in Kansas. HAWK is also used for some case management functions. KDHE staff have full access to HAWK data. Until recently, local health departments could only view records of patients from their respective counties.

Issue

Originally, the HAWK system was designed to give each county access to its own reportable disease records. This presented a problem for the state and local health departments when working with diseases that are common in migratory populations, such as TB. To remedy this, KDHE

[6] HIPAA Privacy Rule and Public Health Guidance from CDC and the U.S. Department of Health and Human Services, 2003. http://www.cdc.gov/mmwr/preview/mmwrhtml/su5201a1.htm.

[7] HAWK is not an acronym; it is the formal name of the system.

[8] NEDSS. A broad initiative to use data and information systems standards to advance the development of efficient, integrated and interoperable surveillance systems. http://www.cdc.gov/nedss/BaseSystem/NEDSSRequirements.pdf

initiated a policy to give all Kansas counties read-only access to TB data across the state. The guidelines for access to and use of the TB data in the HAWK system were formalized in an opt-out Memorandum of Understanding (MOU) with each county in Kansas.

To examine the benefits of increased use of the HAWK system and to further enhance TB management, KDHE formed a partnership with the Medical Director of the Student Health Center at Kansas State University (KSU). He and his staff were given direct access to the HAWK system in order to review TB records already entered and to enter in any cases of TB infection or active disease that they identified through the student health center. This particular physician was chosen for the pilot project because of a history of close work with the local health department on TB issues and because most of the reported TB infection and disease cases in that county were patients identified through the student health center.

The physician and his staff were given only access rights to view TB records for the county where the KSU health clinic is located. The design limitations of HAWK meant that the KDHE could only add the physician as a user by giving him "county staff-level" access. As a result, he would be able to see all TB records that the county health department staff entered into HAWK, even those records that did not belong to his patients. A MOU was created to set guidelines for the physician's new level of access requiring the physician to respect the confidentiality and privacy issues involved.

At the time that the parties were to sign the MOU, the local public health department requested written confirmation that no HIPAA Privacy Rule regulations were being violated through this approach. Amy Biel, MPH, Surveillance Coordinator and HAWK Project Manager in the KDHE, sought this written advice from the Department of Health and Human Services (DHHS) as well as CDC. Beverly Dozier, JD, CDC's Acting Privacy Rule Coordinator (and now CDC's Privacy Rule Coordinator), responded to the KDHE request with a written explanation that the activity described clearly fits within the permitted uses and disclosures of the HIPAA Privacy Rule.

HIPAA Effect

Kansas' HIPAA related questions included: 1) How can data in HAWK be shared across counties without violating HIPAA? 2) Does sharing HAWK data with a private physician violate any HIPAA regulations?

The Privacy Rule regulates PHI disclosed by a covered entity to a public health authority, but not vice versa. KDHE, a public health authority by definition, is therefore permitted to conduct authorized public health activities such as giving a covered entity access to the data entered in its HAWK system.[9] Furthermore, the Rule recognizes the responsibility of public health authorities to monitor health-related data, as is stated: "a public health authority is authorized by law to collect or receive [PHI] for the purpose of preventing or controlling disease, injury, or disability."[10] The HIPAA regulations would have an effect, however, on the opposite direction of data flow: The physician is only permitted to report the minimum necessary TB data into the system. If the physician disclosed more information than the minimum necessary as defined by the HIPAA Privacy Rule, then this would be in violation of the Rule.[11]

Conclusion

Two major hurdles have been overcome: cross-county data sharing and physician access to county-level data. First, KDHE successfully gave counties access to statewide TB data. Counties in Kansas are now able to access read-only versions of other counties' TB data. This has improved efforts regarding continuity of care in migratory populations, many of which are farm worker populations whose locations change with each season.

Secondly, KDHE is moving forward with the physician-access pilot project. According to Amy Biel, "Obviously we want to expand this

[9] Consistent with section [45 CFR 164.501]
[10] Consistent with section [45 CFR 164.512 (b)(1)(i)]
[11] Consistent with section [45 CFR 164.502 (b)(1)]

so that more physicians out in Kansas can use this system for reporting diseases to us. But if we couldn't resolve it the first time we tried to do it, we knew we weren't going to get anywhere. So this was a real hurdle for us, but thanks to Beverly [Dozier], we were able to solve it relatively painlessly."

According to Phil Griffin, Director of the Tuberculosis Control Program in Kansas, "We were trying to roll all this out about the same time (November-December 2002) as the major HIPAA guidelines were coming into play and so everybody was fearing the 'big monster.' But fortunately, at this point, we've been able to meet all those demands. It is very helpful to have the assistance of CDC in giving the guidance that, yes, in fact, the things we were looking to do were permitted by the rule."

Pennsylvania

System Overview

Pennsylvania discussed two methods of data sharing: data that can be shared at the research level and data that is shared at the public health investigation level. Research level data are described as data necessary for research analyses, which are shared with individuals outside of PA-DOH and county-level staff, that includes identifiers, or information that identifies or provides a reasonable basis to believe it can be used to identify an individual.[12] Data shared at the public health investigation level are accessible to PA-DOH staff and county-level staff on a regular basis, generally through PA-NEDSS.

Pennsylvania has a process by which researchers can access department data from the cancer registry, vital statistics registry, and their communicable disease system. Identifiers are not included in most requested data sets. However, some covered entities, including academic and teaching institutions, are frequent requesters of identifiable data for research purposes.

Pennsylvania's approval system for the release of identifiable data consists of a combination of Institutional Review Board (IRB) approval and a Pennsylvania Department of Health (PA-DOH) protocol.[13,14] The process is intentionally stringent to ensure that entities requesting data are carefully screened and have a legitimate public health need for identifiable information. A requester must first show proof of IRB approval from the institution. For example, a researcher from the University of Pennsylvania must gain approval from the University of Pennsylvania IRB before approaching PA-DOH for access to identifiable data. If a requester's institution has not established an IRB, the requester must gain approval through the PA-DOH IRB. Once IRB approval has been granted, the requester must follow the PA-DOH application protocol for access to identifiable data.

The second method of data sharing described for PA-DOH is that of public health investigations. Pennsylvania uses its own version of NEDSS, commonly referred to as PA-NEDSS to collect information for public health use. This system establishes a real-time, secure communication link between laboratories, hospitals, individual medical practices, and the PA-DOH. Providers have immediate access to any information they enter in PA-NEDSS, as well as any laboratory test information ordered for their patients. The laboratories, however, only have access to laboratory reports and are restricted from accessing any provider information. Public health investigators, as a part of PA-DOH, have access consistent with their positions, duties, and geographic areas of responsibility. Public health investigators have access to provider information and laboratory data, as well as the ability to add information.

PA-DOH conducted a HIPAA compliance review prior to the official HIPAA compliance date. Ernst and Young accounting consultants reviewed Pennsylvania's protocols and verified

[12] Consistent with section [45 CRF 164.501]

[13] Bureau of Health Statistics and Research. "Application for Access to Protected Data," Pennsylvania Department of Health. May 2002.

[14] Bureau of Epidemiology. "Data Confidentiality Policy," Pennsylvania Department of Health. September 2003.

that the state's practices were already HIPAA compliant. There are, however, issues that arose after the HIPAA rules took effect that have affected PA-DOH.

Issue

PA-DOH's data sharing protocol limits provision of information only to those cases where PA-DOH deems the information necessary. There are two recent cases that exemplify the data sharing methods that are tailored to give access to only selected data.

The first example is an outbreak of Hepatitis A in Western Pennsylvania in 2003. Attending to all aspects of the large outbreak became overwhelming for the staff. This prompted Joel Hersh, MEd, MPA, Director of Epidemiology at PA-DOH, to approve access for investigators from other geographic areas within Pennsylvania's public health community to assist with the investigation. Public health authorities in Pennsylvania shared hepatitis A data with other local public health authorities for public health purposes, including data analysis and case investigations (standard uses and disclosures for public health activities).[15] Privileges were revoked once the investigation was complete and the outside investigators no longer had a need to access that level of data.

Another example that illustrates access to only selected data is stringency concerning the release of small cell data. Small cell issues refer to the concern that individuals can be identified from non-identified statistical data when there are few people with the same characteristics in the population; this raises data privacy concerns related to the Rule. Since Pennsylvania has a number of small, rural communities, small cell issues are significant, especially with sensitive disease processes such as HIV/AIDS. Because of the possibility of identification, data regarding HIV/AIDS in these populations is not released for the protection of individual rights. To continue protecting this information, Pennsylvania has taken the position, even in the aggregate, that they will not release cells representing fewer than five cases. (Note: A number of states are grappling with small cell issues. The National Association of Health Data Organizations is currently developing a matrix of established approaches to this issue.)[16]

Additional Challenges

One challenge related to the HIPAA rule in Pennsylvania is further development of the PA-NEDSS system to introduce syndromic surveillance. Syndromic surveillance refers to the systematic gathering and analysis of pre-diagnostic health data to rapidly detect clusters of symptoms and health complaints that could signal an outbreak of infectious disease or other conditions.[17] PA-NEDSS data are organized by patient identifiers. The current reporting system, however, does not give PA-DOH direct access to identifiable information for syndromic surveillance data, which creates a barrier to rapid response; PA-DOH must make a request to the reporting facility, which then must connect the data to the correct identifiers. Identifiers are not sent automatically to PA-DOH with this syndromic surveillance data because a diagnosis for a reportable disease (which requires identifiers) has not yet been established at the time of surveillance. For example, data sent to PA-DOH detailing a rise in gastrointestinal illness cases in a hospital would not include patient identifiers until the cause of illness is diagnosed as a reportable disease.

HIPAA Effect

The subject of public health research under the HIPAA Privacy Rule is addressed in the DHHS report, *Protecting Personal Health Information in Research – Understanding the HIPAA Privacy Rule*.[18] Collecting information for research has very different requirements under the HIPAA Privacy Rule than collecting information for public health purposes. For

[15] Consistent with section [45 CFR 164.512]

[16] For more information on NAHDO, visit http://www.nahdo.org

[17] CDC website, Division of Public Health Surveillance and Informatics. Syndromic surveillance: An applied approach to outbreak detection. Retrieved on October 15, 2003 from http://www.cdc.gov/epo/dphsi/syndromic.htm

[18] Department of Health and Human Services. Protecting Personal Information in Research -- Understanding the HIPAA Privacy Rule. Department of Health and Human Services. Washington, D.C.: 2003.

example, an IRB is required when systematic investigation is ongoing such as research development, testing, and evaluation designed to develop or contribute to generalizable knowledge.[19] The majority of public health activities are based on scientific methods and data collection similar to those in research but are not designed to contribute to generalizable knowledge.

Collecting information from covered entities via the PA-NEDSS system is acceptable under the HIPAA Privacy Rule.[20] The PA-NEDSS system was designed with the flexibility to allow and disallow rights to users who should or should not have access. Additionally, PA-NEDSS provides physicians or providers access to reports of the information they send to PA-DOH. This electronic database of patient information is a service that provides some incentive for physicians to assist with public health data sharing efforts.

Conclusion

At the research level, academic and teaching institutions are given access to identifiable information if they gain IRB approval and successfully complete the PA-DOH protocol. And providers can access an organized database of their patients' information through PA-NEDSS, which is also protected by security measures, such as password protection. The private sector providers that report to the PA-DOH are cooperating in submitting reportable information, or data required by state law, and PA-DOH is working to secure additional non-traditional types of information, such as early detection data.

South Carolina

System Overview

The South Carolina Office of Research and Statistics (ORS) within the South Carolina Budget and Control Board has developed an Integrated Data Warehouse (IDW) that allows for data searches across state agencies, private healthcare providers, health plans, behavioral health systems, and claims systems. The ability of the IDW to incorporate new data systems is based on a multi-phase approach to securing access to information. Differing approaches were necessary because of the complexity of confidentiality prescriptions on datasets included in federal and state laws, federal and state programmatic mandates, business privacy regulations, and sometimes local laws and programmatic mandates. Data from 14 state agencies are included in the IDW via state law[21] requiring the submission of data under a cooperative Memorandum of Agreement (MOA).

Private databases, emergency department, inpatient hospitalization, home health, and ambulatory surgery are provided under separate legislation.[22] All-payer healthcare databases and other selected providers, such as free clinics, supply data under business associate agreements.[23] ORS' ability to assemble these data using a statistical "patient linker number," or unique identifier, provides security for the agency and patients and reduces the obstacles for data access and release.

Box 2. South Carolina State Agencies whose data are included in the integrated database

- Department of Alcohol and Other Drug Abuse Services;
- Commission for the Blind;
- Division for the Review of Foster Care of Children;
- Department of Education;
- Department of Health and Environmental Control;
- Department of Health and Human Services;
- Department of Juvenile Justice;
- Department of Mental Health;
- Department of Disabilities and Special Needs;
- School for the Deaf and the Blind;
- Department of Social Services;
- Department of Vocational Rehabilitation;
- Division of Continuum of Care;
- Department of Corrections and Probation, Parole and Pardon Services.

[19] Consistent with section [45 CFR 501]
[20] Consistent with section [45 CFR 164.512 (b)(1)(i)]
[21] South Carolina Budget Proviso 72.21.(GP: SC Health & Human Services Data Warehouse), 2003.
[22] Code of Laws of South Carolina, 1976, Section 44-6-170, 175 and 180, as amended.
[23] Consistent with section [45 CFR 164.308 (a)(8)(b)(1)]

South Carolina's IDW connects information across a number of different systems, including legal/safety services, social services, claims systems, all-payer healthcare databases, behavioral health, health department data, education data, disease registries, and other state support agencies information.[24] Records are organized by statistical linker numbers that are assigned to each individual in the database, allowing each patient's data to be linked.

Requests for data from one agency, private database or healthcare payer, or other healthcare provider are handled within each entity. For instance, the Department of Mental Health would process all requests for mental health data. If a request is made for data held by multiple state agencies or entities operating under a business associate agreement, each agency/entity involved must give permission to release its section of the requested data using the data release policies proscribed by law, federal or state program mandates, or other data release requirements established by the entity. Generally, in cases of a multiple agency or entity request, the request is first sent to ORS. However, any involved entity may begin the process.

Private sector data (i.e., hospital inpatient, outpatient surgery, emergency, and home health data) are processed and approved by the state's Data Oversight Council (DOC) established by state legislation and comprised of government, businesses, providers, and payers.[25] The DOC governs the release of private sector data using a data release protocol, which includes an application calling for a written statement of use of the data requested, type of data releases, protection for the privacy of the data, and a Confidentiality Contract delineating the approved uses of the data.

Once approval is obtained to track information across several different databases, there are two options for data release. The statistical data set at the person-level may be released to the requester, or ORS can perform analyses specified by the requester and release the results. The latter process is performed by individuals specializing in the use of the data at ORS, thereby increasing the consistency of the analyses. The releasing agencies, entity, or the DOC may include conditions to the release. For example, an agency may require a review of the analysis before the requester releases information obtained from the data.

According to Pete Bailey, MPH, Chief of the Health and Demographic Section of ORS, "This process has been running for quite a while, and it has been very good. Everybody is learning the great things you can do with the integrated data."

For example, ORS has been able to use the integrated system to conduct data analyses dependent on several agencies, all-payer databases, and private data. For example, information was recently requested regarding the overlap of suicide cases and emergency room visits in a specified six-month time frame. ORS was able to access the death records, emergency room data, and mental health center data to fulfill the request. According to Buddy Hudson, MPH, Director of Public Health Statistics and Information Services at DHEC, the state has just begun to scratch the surface of what can be done in the way of prevention strategies for public health with these new capabilities.

Future improvements include development of a web-based data warehouse. The data would be stored in sets called "cubes." A cube is part of a software program used by South Carolina that organizes a set of data specifically to increase the ease of data analysis. The first cube prototype is almost complete and includes information on maternal and child health, and involves social services, Medicaid, all-payer inpatient, and vital records data. South Carolina is also moving toward creating a client management system to enhance continuity of care. This type of system would track any services provided to a patient by the 14 state agencies and could create HIPAA-related

[24] *South Carolina Data Warehouse*. South Carolina Department of Health and Environmental Control, 2004.
[25] Code of Laws of South Carolina, 1976, Section 44-6-170, 175 and 180, as amended.

questions in the future regarding increased access to health data.

HIPAA Effect

To ensure that the state's public health system continues to receive necessary health information, South Carolina passed a law requiring covered entities to send information to the appropriate state agencies. According to HIPAA, "as a federal regulatory standard, the Privacy Rule preempts only those contrary state laws relating to the privacy of individually identifiable health information that have less stringent requirements or standards than the Privacy Rule (i.e., more stringent laws remain in effect)".[26] South Carolina's law was written to be more stringent than HIPAA, thereby preempting the related sections of the HIPAA Privacy Rule.

The law also states that because the agencies maintain control over the data, it is their responsibility to send that information to ORS for data integration. ORS has a formal MOA with each agency to maintain the confidentiality of the data. This is enhanced by the long maintained trust between South Carolina's citizens and the state's public health system, which is grounded in treating patient privacy as a top priority.

Mary Tyrell, HIPAA Privacy Officer for the South Carolina ORS, stated that even though HIPAA was not designed to limit public health efforts, one potentially unintended consequence has been the perception of data requesters that there is an increase in paperwork necessary to obtain permission to access the integrated database. "Some researchers have given up before applying because of this perception. Reality is that access can be obtained in a timely fashion."

Conclusion

South Carolina's IDW has proven to be an effective method of information storage and analysis for the state's public health system. Denise Love, RN, MBA, Executive Director of the National Association of Health Data Organizations (NAHDO) stated, "We look at South Carolina as a model for other states. They have worked through the data sharing agreements with their sister agencies and really do maximize the utility of their data. Not just public health data, but all data. I also appreciate how it has streamlined the reporting process for providers and eliminates redundant and dual reporting."

Integrated databases are also of benefit to the clinical sector, saving them the work of developing their own data organization system, and giving them the ability to access their patients' data and enhance continuity of care. The state has shown that integrated data exchange and individual privacy can be balanced when those involved with the public health system work in coordination and cooperation with one another.

Key Findings

Kansas, Pennsylvania, and South Carolina have all encountered issues since the implementation of the HIPAA Privacy Rule. These states have designed their systems to overcome many of these challenges. The resolutions of these issues range from similar in nature to great variance due to state specific needs.

Similarities in Approaches

Each of the states asserted that, as a result of the HIPAA Privacy Rule implementation, they have encountered some resistance from covered entities regarding data sharing. To address these challenges, all three states have dedicated time and resources to educating covered entities about the fact that the Privacy Rule fully allows them to share PHI with public health authorities.

Each state described its protocols for the release of information held by public health departments and specifically addressed how PHI is released in this context. Kansas developed an MOU which listed guidelines for access and use of the TB data that is currently shared across counties. Kansas also described its initiative to share data with physicians and its implications for PHI disclosure, which were also addressed with an

[26] Consistent with section [45 CFR 160.202]

MOU. Pennsylvania's data release process is guided by the state's Application for Access to Protected Data[27] and review process. The South Carolina release process is based upon an agency-specific review of the data in question (i.e., the Department of Mental Health would review any requests for mental health data).

Benefits and ease of use for covered entities are also common features in all three state systems. For example, the Kansas HAWK system now allows for one physician to view county-wide TB data, giving the physician a broader perspective of the county's health standings regarding TB. The Pennsylvania system allows physicians to access an electronic database of medical and laboratory diagnoses for their patients. Both KDHE and PA-DOH are working to expand these programs. South Carolina developed a DOC to regulate disclosures of private sector data and to maintain the integrity of data stored in the state's IDW, ensuring that the privacy of covered entities' patients is maintained.

The states differ in their systems' guidelines regarding accessibility of data. For example, Pennsylvania built its data collection system with the flexibility to allow and disallow rights of users to access data. This contrasts with Kansas' approach, where all counties have continuous, read-only access to other counties' TB data. Both approaches are allowable under the HIPAA Privacy Rule. However, the levels of each state's control differ between the two systems.

Another difference is the level of integration of data sets. Pennsylvania and Kansas have developed tracking systems and are improving public health investigation and prevention measures. South Carolina has designed its system, as well as written its law, with the intent to integrate the reported data.

[27] Bureau of Health Statistics and Research. "Application for Access to Protected Data," Pennsylvania Department of Health. May 2002.

Major Themes

Several themes emerged related to data sharing with covered entities under the HIPAA Privacy Rule.

HIPAA Implementation Issues for PHI

With the HIPAA Privacy Rule in effect, some covered entities have been reluctant to continue to send information to public health. Many state and local public health departments have spent time and resources educating and working with covered entities to ensure that data which have been traditionally collected, as well as important new data sets, will be sent to public health departments.

While the Privacy Rule clearly states that PHI may be sent to a public health authority, covered entities are concerned that they will be held accountable for this information once it leaves their control. The word "may" in this context has created obstacles for a number of state public health departments.

States have suggested that modifying the HIPAA Privacy Rule to clarify that this type of information exchange is acceptable would ease confusion. Kansas was able to address concerns by obtaining clarification in writing from CDC and sharing it with the concerned parties.

Even if the language in the Rule is clarified regarding information that can be sent to public health authorities, covered entities still have the administrative responsibility to disclose that health information to public health personnel who ask for it. DHHS allows covered entities to streamline disclosure reports for requesters.[28] There also have been suggestions that the disclosure requirements for information sent to public health authorities be taken out of the HIPAA Privacy Rule. The Privacy Rule allows DHHS to make amendments to the Rule on an annual basis.

[28] http://www.hhs.gov/ocr/hipaa

Working Well with Covered Entities

Covered entities are heavily involved in data collection for public health through their routine interaction with patients in the community. It is important for public health to consider how to facilitate the flow of information with covered entities. South Carolina's integrated data system could provide information of interest to covered entities.

Additionally, Pennsylvania has described two examples of services that they plan to provide to make information sharing easier for covered entities. The first is giving tracking capabilities to covered entities (including receipt of lab reports that they have ordered), and allowing the covered entity to easily access the information they are reporting to PA-DOH. Another is to automate laboratory reporting by providing each Pennsylvania hospital with a computer server. The server would route laboratory reportable disease data directly into PA-NEDSS. These two services save the covered entities the work involved in designing their own systems, and increase the covered entities' compatibility with PA-NEDSS.

No One Best Approach

As exemplified by the three different state approaches, implementation of the HIPAA Privacy Rule and approaches to data sharing differ from state to state. State public health department needs vary and other federal and state laws need to be taken into account. State laws on privacy may be more stringent than the HIPAA Privacy Rule, thereby preempting HIPAA. For example, Pennsylvania's laws regarding data access have stronger protections than the HIPAA Privacy Rule. As a result, the state was able to leave its earlier-developed system intact. Each state has developed the approach that best meets its needs regarding infrastructure, state laws, and other concerns, while adhering to the HIPAA Privacy Rule.

Protecting the Privacy of Individuals – A Public Health Priority

Once PHI is sent to public health authorities, it is no longer covered under HIPAA. However, public health departments adhere to policies, procedures, and state laws that protect the privacy of individuals. South Carolina's law specifically lists topics that should be addressed in MOAs between agencies and ORS, including (but not limited to) "the confidentiality of client information; the conditions for the release of data that may identify agencies, departments, divisions, programs and services; any restrictions on the release of data so as to be compliant with state and federal statutes and regulations on confidentiality of data; conditions under which the data may be used for research purposes; and any security measures to be taken to ensure the confidentiality of client information." States understand that protecting the privacy of individuals is of critical importance and take this responsibility very seriously.

Potential for Integrated Information

As the South Carolina approach shows, the ability to integrate information across a number of data systems enhances public health knowledge and presents opportunities to develop more effective and targeted interventions. Buddy Hudson of the South Carolina DHEC says there is great potential for protection of health as a result. Efforts to integrate systems will have to be continually monitored to ensure that privacy issues are considered.

Sharing Experiences Across States is Valuable

Finally, as ASTHO has worked with a number of states to explore HIPAA issues, it consistently receives feedback that sharing approaches to HIPAA implementation among state public health staff is important. The ability to learn from other states was frequently cited in a July 2003 survey of HIPAA Task Team members when asked what guidance or technical assistance would facilitate HIPAA compliance efforts. Learning from states with similar structures was cited as an important aspect of guidance or assistance. Working with CDC HIPO and others, ASTHO hopes to continue to provide states and their partners with assistance they need to effectively implement the HIPAA rules.

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 HIPAA.

Pete Bailey, MPH, Chief of Health and Demographic Section, Office of Research and Statistics, South Carolina Budget and Control Board. Personal Communication January 27, 2004.

Amy Biel, MPH, Surveillance Coordinator, Bureau of Epidemiology and Disease Prevention, KDHE. Personal Communication January 27, 2004.

Beverly Dozier, JD, Privacy Rule Coordinator, CDC. Personal Communication January 27, 2004.

Phil Griffin, BBA, CPM, Director of Tuberculosis Control Program, Bureau of Epidemiology, PA-DOH. Personal Communication January 27, 2004.

Joel Hersh, MEd, MPA, Director, Bureau of Epidemiology, PA-DOH. Personal Communication January 27, 2004.

James G. Hodge, Jr., JD, LLM, Executive Director, Center for Law and the Public's Health, Johns Hopkins Bloomberg School of Public Health. Personal Communication January 27, 2004

Buddy Hudson, MPH, Director, Public Health Statistics and Information Services Division, South Carolina DHEC. Personal Communication January 27, 2004.

Robin Ikeda, MD, MPH, Associate Director of Science, Epidemiology Program Office, CDC. Personal Communication January 27, 2004.

Denise Love, RN, MBA, Executive Director, National Association of Health Data Organizations. Personal Communication January 27, 2004.

Mary Tyrell, HIPAA Privacy Officer, South Carolina Office of Research and Statistics. Personal Communication March 3, 2004.

References

Office for Civil Rights. Department of Health and Human Services. Title 45 of the Code of Federal Regulations Parts 160 and 164. Available at www.dhhs.gov/ocr/combinedregtext.pdf

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

CDC. Guidelines for defining public health research and public health nonresearch. Available at http://cdc.gov/od/ads/opspoll1.htm.

HIPAA Privacy Rule and Public Health Guidance from CDC and the U.S. Department of Health and Human Services, 2003. Available at www.cdc.gov/mmwr/preview/mmwrhtml/su5201a1.htm.

Bureau of Health Statistics and Research. "Application for Access to Protected Data," Pennsylvania Department of Health. May 2002

Bureau of Epidemiology. "Data Confidentiality Policy," Pennsylvania Department of Health. September 2003.

South Carolina Budget Proviso 72.21.(GP: SC Health & Human Services Data Warehouse), 2003.

Online Resources

Federal Government Resources

Center for Disease Control and Prevention-Privacy Rule Guidelines
www.cdc.gov/privacyrule

Centers for Medicare and Medicaid Services
www.cms.gov/hipaa

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

Indian Health Service
www.ihs.gov/AdminMngrResources/HIPAA/index.cfm

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

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

National Health Information Infrastructure
www.health.gov/ncvhs-nhii/

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

State Government Resources

Kansas www.kdhe.state.ks.us/

Pennsylvania
www.dsf.health.state.pa.us/health/site/default.asp

South Carolina www.scdhec.net/

Associations, Nonprofit Organizations, and Academic Resources

American Hospital Association-HIPAA
www.hospitalconnect.com/aha/key_issues/hipaa/index.html

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/

Joint Healthcare Information Technology Alliance
wwwjhita.org/

National Association of Health Data Organizations
www.nahdo.org/

National Association of Insurance Commissioners
www.naic.org/1privacy/initiatives/health_privacy.htm

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

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

Stanford University Medical School-HIPAA
http://irt.stanford.edu/privacy/hipaa/

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

Association of State and
Territorial Health Officials

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