PRIVACY AND PUBLIC HEALTH PRACTICE SERIES

Information Management for State Health Officials

The Impact of the HIPAA Privacy Rule on Syndromic Surveillance

ASSOCIATION OF STATE AND TERRITORIAL HEALTH OFFICIALS

The Impact of the HIPAA Privacy Rule on Syndromic Surveillance

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.

Syndromic surveillance is a relatively new undertaking on the part of state public health departments. While traditional health monitoring focuses on tracking diagnosed disease and conditions, syndromic surveillance centers closely on indicators of disease, such as fever, rash, gastrointestinal illness, and respiratory conditions. Several states have already initiated syndromic surveillance through their departments of health, while other states are just beginning to build the framework for their monitoring systems. This report highlights issues encountered by individuals who have different levels of exposure to and experience with syndromic surveillance in efforts to provide guidance to states working to improve their syndromic surveillance systems.

Key Findings

Key findings or themes resulting from discussions with these states regarding syndromic surveillance and the HIPAA Privacy Rule include:

1. Determining Authority to Collect Syndromic Surveillance Data

Public health authorities have encountered difficulties in collecting data from covered entities. Some believe that this issue would be alleviated if syndromic surveillance was mandated by state law, thereby officially giving states the authority to collect the data. Several states have modified their statutes in order to conduct effective syndromic surveillance, while others have used education and the support of Joint Commission on Accreditation of Healthcare Organizations (JCAHO) and the Health Resources and Services Administration (HRSA) to explain to covered entities the necessity of collecting syndromic surveillance data.

2. Understanding the Rights of a Public Health Authority

HIPAA states that the public health authority has the power to collect that data requested from a covered entity; however, varied interpretations of the Rule have created difficulty for the success of syndromic surveillance. Covered entities have stated that data is generally withheld in the interest of patient privacy and data security, reducing the likelihood of accurate syndromic surveillance. States have noted that security is always one of the top priorities and is generally one of the first aspects of syndromic surveillance plans to be addressed.

3. Deciding Whether to Collect Identified Versus De-identified Data

When performing syndromic surveillance, it is important to note the difference between collecting identifiable information and de-identified information. When syndromic surveillance is performed without identifiable information, there are no HIPAA implications. However, many syndromic surveillance systems involve the disclosure of identifiable health information by covered entities. The practice of collecting identified information increases HIPAA involvement in syndromic surveillance (covered entities would be responsible for accounting for these disclosures), but also increases the efficiency of the system. When identifiable information is included in data

reports, public health authorities avoid extra steps in going back to covered entities for further information during the investigations of aberrations in syndromic surveillance data.

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.

About ASTHO

The Association of State and Territorial Health Officials 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 the HIPAA Privacy Rule implementation. The purpose of the HIPAA Task Team (HTT) is to identify issues that primarily impact 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 at Georgetown and Johns Hopkins Universities, to continue the HTT forums and to write issue reports around the topics considered in each forum.

The topic for this second issue report is: "The HIPAA Impact on Syndromic Surveillance." The issue report includes a review of the major HIPAA privacy issues that state public health departments may encounter when conducting syndromic surveillance. The information in this paper is largely based on presentations made by the following people at the March 2004 HTT forum teleconference: James G. Hodge, Jr., JD, LLM; Richard Melton, DrPH, Deputy Director of the Utah Department of Health; and James Jerry Gibson, MD, MPH, Director, Bureau of Disease Control, South Carolina Department of Health and Environmental Control.

Introduction

Syndromic surveillance is a relatively new undertaking on the part of state public health agencies. While traditional public health surveillance focuses on tracking diagnosed disease and conditions, syndromic surveillance centers closely on indicators of disease, such as fever, rash, gastrointestinal illness, and respiratory conditions. Several states have already initiated syndromic surveillance through their public health agencies, while other states are just beginning to build the framework for their monitoring systems. This ASTHO HIPAA Task Team teleconference and this paper highlight issues encountered by individuals who have different levels of exposure to and experience with syndromic surveillance and provide guidance to states working to initiate or improve their syndromic surveillance systems.

Summary of HIPAA Task Team Teleconference Presentations

James G. Hodge, Jr., JD, LLM, Executive Director for the Center for Law and the Public's Health, introduced the concept of syndromic surveillance, defined as "a 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."[1] Mr. Hodge noted several legal issues underlying the HIPAA Privacy Rule as it related to the practice of syndromic surveillance by state and local public health agencies. These included: state or local public health agencies' statutory or legal authorities while collecting identifiable data for public health purposes, the role of public health entities in determining appropriate information release during syndromic surveillance activities, and the circumstances under which a covered entity can deny the requested information to a public health authority.

Dr. Richard Melton, Deputy Director of the Utah Department of Health (UDOH), shared the Department's unique experiences with the syndromic surveillance that took place during the Salt Lake City Olympics and how they relate to the HIPAA Privacy Rule. The state initially encountered some barriers during the Olympics, but eventually UDOH modified its statutes to require collection of information from hospitals for special purposes. After this was completed, UDOH implemented three reporting systems to successfully conduct syndromic surveillance.

Dr. Jerry Gibson, Director, Bureau of Disease Control, South Carolina Department of Health and Environmental Control (DHEC), discussed a 9-question survey that he and Dan Drociuk, Director, Bioterrorism Surveillance and Response Program, South Carolina DHEC, conducted. The survey, "Survey of Bioterrorism Directors on Privacy, Confidentiality, and HIPAA issues in Syndromic Surveillance," was distributed to state and city CDC Focus Area B[2] directors and state epidemiologists. This survey was conducted with the intention of clarifying any misinterpretations of the HIPAA privacy provisions which may obstruct the disclosure of regular surveillance data by covered entities to syndromic surveillance systems.

What is Syndromic Surveillance?

Syndromic surveillance traditionally refers to the monitoring and collecting of pre-diagnosis health data. Syndromic surveillance is used as an indicator of an outbreak that might warrant further investigation.[3] For example, syndromic surveillance includes reviews of routinely gathered information on gastrointestinal illness, rash, and fever. Syndromic surveillance systems often include the disclosure of protected health

[1] CDC website, Division of Public Health Surveillance and Informatics (2002). Syndromic Surveillance: An applied approach to outbreak detection [On-line]. Available: http://www.cdc.gov/epo/dphsi/syndromic.htm.

[2] CDC's Focus Area B covers "Surveillance and Epidemiology Capacity"; http://www.bt.cdc.gov/planning/continuationguidance/pdf/guidance_intro.pdf

[3] Mostashari F, Hartman J. *Syndromic surveillance: A local perspective.* J. Urban Health. 2003 Jun; 80 (2Suppl 1): i 1-7.

information[4] (PHI) by covered entities,[5] which has spurred legal concerns regarding the role of the HIPAA Privacy Rule in syndromic surveillance.

The Impact of HIPAA on Syndromic Surveillance

Statutory and Legal Authority to Collect Data

Syndromic surveillance raises several issues related to the HIPAA Privacy Rule. According to the HIPAA Privacy Rule, covered entities may disclose PHI for public health activities and purposes including "information 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 and death, and the conduct of public health surveillance, public health investigations, and public health interventions.[6] Thus, the Privacy Rule allows public health authorities to collect PHI without written authorization for various legally-authorized purposes, such as surveillance.

Although disease reporting and other surveillance activities are specifically authorized or required in every state, syndromic surveillance does not always fit neatly within general surveillance authorizations, as it may not involve diagnosed reportable conditions. A survey developed by Jerry Gibson and Dan Drociuk of South Carolina's DHEC showed that 35% (n=11) of respondents considered recommending changes to their state reporting statutes to include syndromic surveillance systems. However, 65% (n=20) of the respondents noted that they would not consider recommending modifying their state statutes until more analyses on the value of these systems had been completed.[7]

Utah chose to amend its statutory or regulatory provisions to specifically authorize syndromic surveillance. For the winter 2002 Olympics in Salt Lake City, UDOH modified its statute that requires the collection of information from hospitals for special purposes. The "Detection of Public Health Emergencies Act," which was passed in preparation for the Olympics, requires that a health care provider "report to the Department any case of any person who the provider knows has a confirmed case of, or who the provider believes in his professional judgment is sufficiently likely to harbor any illness or health condition that may be caused by: bioterrorism, epidemic, or pandemic disease; or novel and highly fatal infectious agents or biological toxins which might pose a substantial risk of a significant number of human fatalities or incidences or permanent or long-term disability."[8] UDOH strengthened its statute to facilitate follow-up data collection if necessary; the previous statute had only allowed UDOH to follow-up on diagnosed conditions, not syndromic data.

Once the statute was amended, UDOH was able to collect syndromic information through various reporting systems: the Urgent Care Surveillance (UCS) system; Salt Lake Organizing Committee (SLOC) Medical Services encounters; and Real-time Outbreak Data Surveillance (RODS) system. Scientists from the University of Utah, Intermountain Health Care (IHC), and the University of Pittsburgh implemented all three systems to help minimize the effect of an intentionally caused disease outbreak.

The Urgent Care Surveillance system included a manual and an electronic reporting component that monitored for syndromes in 43 facilities across six local health departments (LHD). The LHD staff reviewed complaint logs and categorized them through chart reviews for

[4] Protected health information - individually identifiable health information as defined by the HIPAA Privacy Rule [45 CFR 160.103]

[5] Covered entity - health plan, healthcare clearinghouse, or health care provider as defined by the HIPAA Privacy Rule [45 CFR 160.103]

[6] Consistent with section [45 CFR 164.512(b)(1)(i)]

[7] Drociuk, D. & Gibson, J. (2003). Experience of Syndromic Surveillance Systems with Issues of Patient Privacy & HIPAA. Available: www.syndromic.org/pdf/con2-PG-7b.pdf. (Question 3b: "Considered adding SSS to state reporting statutes?")

[8] Detection of Public Health Emergencies Act, Utah. Stat. Ann. 26-23B-101 et esq. (2002)

syndromic classification in 19 facilities. UCS transmitted this data to UDOH each morning via email, and a report was submitted by LHD staff for the previous 24 hours each afternoon.[9] This system reported chief complaints at registration that were based on keywords (e.g., "cough") and analyzed any data aberrations. The electronic reporting component of the UCS system included 19 IHC InstaCares/KidsCare facilities. It also monitored one emergency room facility at the University of Utah, where the syndromes were categorized by ICD-9 codes in corresponding electronic medical records.[10]

The second method of surveillance in place was the SLOC Medical Encounters Surveillance System which monitored a multi-specialty clinic located in the Olympic Village. The clinic was staffed by epidemiologists who monitored syndromes against the 17 medical or injury conditions listed on the encounter form and reported the data on a daily basis.[11] This surveillance system proved successful when syndrome peaks signaled an outbreak of influenza in the monitored population.

Lastly, RODS was used in parallel with the other two reporting systems. RODS, an electronic surveillance system, was deployed in 1999 through the University of Pittsburgh and is currently UDOH's main reporting system for conducting syndromic surveillance. The system captures clinical data from multiple health systems under shared data agreements. RODS receives data in real time from existing clinical information systems and then analyzes data from all patients presenting for acute care with chief complaints of diarrhea, rash, respiratory illness, viral illness and noting any other aberrations from the usual patterns. A web-based interface provides access to a geographic information system, graphical analytical tools, and other analytical tools that facilitate rapid investigation of suspicious trends.[12]

Covered entities and public health authorities need clarification on syndromic surveillance's relation to traditional data reporting. A thorough understanding may influence a state's decision on whether or not to modify reporting statutes. Lessons learned from Utah's Olympics experience may help guide other states that are interested in modifying statutes.

Authorizing Data Release and the Rights of a Public Health Authority

Covered entities under the Rule have also posed the question, "Who has the authority to determine what information will be released?" The HIPAA Privacy Rule states that, if public health authorities determine that the requested information is necessary, covered entities may defer to this judgment and provide that data.[13] In the case of syndromic surveillance, covered entities have challenged public health authorities on whether all of the requested information is needed or even allowed under HIPAA. This challenge may result in the covered entities refusing to release requested information to public health authorities, hampering the public health authorities' ability to conduct surveillance.

Questions have also been raised regarding the rights of a public health authority when conducting syndromic surveillance. States maintain that if they have statutory authority to collect health information, covered entities could more easily justify syndromic surveillance disclosures by referring to the state's laws, increasing covered entity compliance. However, it is important to note that the HIPAA Privacy Rule is not a substantive public health statute. The HIPAA Privacy Rule is designed to protect

[9] Gesteland, Per H. Legal Perspectives of Implementing Syndromic Surveillance Systems-Utah Case Study . Available: www.syndromic.org/pdf/con2-PG-7b.pdf.

[10] CSTE website (2002). Public Health Surveillance for the 2002 Olympic Winter Games [On-line]. Available: www.cste.org.

[11] CSTE website (2002). Public Health Surveillance for the 2002 Olympic Winter Games [On-line]. Available: www.cste.org.

[12] Gesteland, Per H., et al (2002). Rapid Deployment of an Electronic Disease Surveillance System in the State of Utah for the 2002 Olympic Winter Games [On-line]. Available: www.health.pitt.edu/rods/LIBRARY/Per.Gesteland.AMIA.2002.Final.pdf

[13] Consistent with section [45 CFR 164.512(b)(1)(i)]

the privacy of national health data; it does not authorize public health authorities to collect data, but simply allows covered entities to supply information to authorities for specified purposes.

An illustrative example shared by Dr. Farzad Mostashari of the New York City Department of Health and Mental Hygiene (NYCDOHMH) concerns a study which was conducted after the New York City blackout of August 2003. During the blackout several different New York City syndromic systems detected an abberation increase in gastrointestinal (GI) illness. To evaluate whether these signals were associated with the blackout, NYCDOHMH designed a case-control study. NYCDOHMH epidemiologists reviewed the hospital GI charts and collected control data by reviewing other emergency department patients' charts. Hospitals questioned the authority of epidemiologists to look at the control patients' data but did not question their right to look at the charts of patients captured by the syndromic system. This authority issue prevented timely data exchange and resulted in a reduced amount of data available for NYCDOHMH during the time the study was conducted.

Clarification is needed around authority-to-collect and mandated syndromic data collection. Varied interpretations can impede data collection and data analyses, as seen in the New York City example. Public health authorities and covered entities would benefit from more guidance around these topics.

Collecting Identifiable Health Information

Maintaining the confidentiality of PHI has impacted how covered entities engage in syndromic surveillance. However, the Rule does not specify the use of identifiable data such as for performing public health surveillance research. As a result, institutions interpret the Rule differently regarding appropriate disclosures. Public health authorities fear that this confusion will prevent covered entities from reporting information necessary for effective syndromic surveillance.

Additionally, the Rule's accounting provision has impacted syndromic surveillance. The Rule states that covered entities are required to account for any disclosures of PHI to public health authorities, discouraging many covered entities from reporting to public health because of the perceived increase in paperwork. Some covered entities have addressed the accounting issue by sending de-identified data or limited data sets, bypassing the accounting requirement.[14]

This type of data exchange is not favorable for public health authorities who may need the identifiable data during syndromic data analyses. However, the Rule states that simplified accounting methods are also acceptable.[15] For example, if a covered entity has made multiple disclosures to the same recipient for the same purpose over the course of one accounting period, the HIPAA Privacy Rule allows the covered entity to provide the following information in response to a request for an account of disclosures: the recipient of the disclosures, the purpose of disclosure, and a description of the PHI routinely disclosed. Additional information required to be reported includes a report of the date of first and last disclosure in an accounting period and the frequency of such disclosures.[16] This type of accounting would increase the efficiency of syndromic surveillance systems from the public health authority's perspective and keep the burden on covered entities to a minimum.

The South Carolina DHEC survey indicated that states ranged from reporting substantial problems to reporting no problems regarding confidentiality and the HIPAA Privacy Rule in syndromic surveillance systems. States noted that problems were caused by covered entities' concerns about violating the HIPAA Privacy Rule, causing them to refrain from reporting syndromic surveillance data. Reductions in

[14] Consistent with section [45 CFR 164.528(a)(1)]
[15] Consistent with section [45 CFR 164.528]
[16] Centers for Disease Control and Prevention. HIPAA Privacy Rule and public health: guidance from CDC and the U.S. Department of Health and Human Services. MMWR 2003; 52 (Supl): [8-9].

reported data also stemmed from covered entities only sharing the "minimum necessary" data or requesting multiple reviews of data prior to its release, hampering timely and effective disease surveillance. Other states, however, reported few problems with maintaining confidentiality. Many of these states noted that they collect aggregate data only, easing covered entities' concerns of breaches in privacy. One respondent limited data collection to date/time, demographics, chief complaint, diagnosis, disposition, and zip code.[17]

In his article, *Syndromic Surveillance Using Minimum Transfer of Identifiable Data*,[18] Richard Platt, MD, Professor at Harvard Medical School, described a syndromic surveillance system currently in development. The National Demonstration Program will focus on collecting aggregated syndromic data on a daily basis, as opposed to the traditional individual-level data reports, thereby increasing patient confidentiality efforts. Over 20 million people will be covered by this system, and each will be assigned to a specific geographic area, increasing public health's ability to monitor abnormal health patterns by location. The covered entity will maintain records of any identifiable information related to the aggregated data, releasing it to the public health authorities only when necessary for disease tracking.[19]

Covered entity reporting of identifiable health information will benefit public health authorities' analyses of syndromic surveillance data. However, some covered entities have been reluctant to send identifiable data because of the HIPAA Privacy Rule's accounting requirement. Further education on the accounting requirement and the importance of identifiable health information to syndromic surveillance may be an appropriate method of overcoming this issue.

Key Findings

The issue of syndromic surveillance and the HIPAA Privacy Rule has sparked many areas of interest among public health authorities and covered entities. The main issues include: determining the authority to collect syndromic surveillance data, understanding the rights of a public health authority, and deciding whether to collect identified data versus de-identified data.

1. Determining State Legal Authority to Collect Syndromic Surveillance Data

Public health authorities have encountered difficulties in collecting data from covered entities. Some believe that this issue would be alleviated if syndromic surveillance was mandated by state law. Several states, including Utah, have modified their statutes in order to conduct effective syndromic surveillance. The DHEC survey addressed the significance of the lack of mandated reporting, however, and found that responses were split. Respondents stated that covered entities have not seen the value in reporting syndromic data, since it is not as accurate as disease diagnoses data. However, education has been effective in convincing the majority of the covered entities that syndromic surveillance does have value. Others noted that syndromic surveillance is a priority for the Joint Commission on Accreditation of Healthcare Organizations (JCAHO) and the Health Resources and Services Administration (HRSA). The fact that these organizations stress the importance of syndromic surveillance may increase the covered entities' likelihood of sharing syndromic surveillance data. Still others stated that the issue should not be framed as increasing support for syndromic surveillance,

[17] Drociuk, D., & Gibson, J. (2003). Experience of Syndromic Surveillance Systems with Issues of Patient Privacy & HIPAA. Available: www.syndromic.org/pdf/con2-PG-7b.pdf. (Question 2: "What has been your experience with confidentiality and HIPAA in Syndromic Surveillance systems?")

[18] Platt, Richard., et al. *Syndromic Surveillance Using Minimum Transfer of Identifiable Data: The Example of the National Bioterrorism Syndromic Surveillance Demonstration Project*. J. Urban Health. 2003 Jun; 80 (2 Suppl 1) 25i-31i.

[19] Platt, Richard., et al. *Syndromic Surveillance Using Minimum Transfer of Identifiable Data: The Example of the National Bioterrorism Syndromic Surveillance Demonstration Project*. J. Urban Health. 2003 Jun; 80 (2 Suppl 1) 25i-31i.

but rather as reinforcing the importance of astute physicians.[20]

2. Understanding the Rights of a Public Health Authority

HIPAA states that a public health authority has the power to request and collect data from a covered entity; however, varied interpretations of the Rule have created difficulty for the success of syndromic surveillance. Covered entities have stated that data is generally withheld in the interest of patient privacy and data security. Multiple responses on the DHEC survey stated that security is always one of the top priorities and is generally one of the first aspects of syndromic surveillance plans to be addressed. One state noted that most outside staff only have access to copies of databases, not the "real" databases, preventing possible data manipulation and reducing security concerns. Eighty-three percent (n=25) answered that they were not concerned about the data security of their systems, and that the current security levels in their plans are adequate.[21]

3. Deciding Whether to Collect Identified Versus De-identified Data

When performing syndromic surveillance, it is important to note the difference between collecting identifiable information and de-identified information. When syndromic surveillance is performed without identifiable information, there are no HIPAA implications. However, many syndromic surveillance systems involve the disclosure of identifiable health information by covered entities. For example, medical practitioners, hospitals, and insurance companies that send health data electronically to public health authorities would be required to disclose this information to individuals if requested. The practice of collecting identified information increases HIPAA involvement in syndromic surveillance, but also increases the efficiency of the system. When identifiable information is included in data reports, public health authorities avoid extra steps in going back to covered entities for further information during the investigations of aberrations in syndromic surveillance data.

Conclusion

As state public health agencies move forward with syndromic surveillance efforts, the experiences of early adopters and those who have studied the related HIPAA privacy issues involved can be a practical planning guide. We have learned from James Hodge about the major issues and questions surrounding syndromic surveillance and the HIPAA Privacy Rule and from Jerry Gibson about varied state experiences with syndromic surveillance. We reviewed the actions taken as a result of Utah's practical experience with the winter Olympics to continue syndromic surveillance as part of the state's public health system. As national syndromic surveillance planning efforts are launched, it will be important to determine the role of states in sending and receiving syndromic data to and from federal agencies. The issues involving collecting PHI become even more challenging in this situation.

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 and syndromic surveillance.

James Jerry Gibson, MD, MPH, State Epidemiologist and Director, Bureau of Disease Control, South Carolina Department of Health and Environmental Control. Presenter on HIPAA Task Team Call, March 19, 2004.

[20] Drociuk, D., & Gibson, J. (2003). Experience of Syndromic Surveillance Systems with Issues of Patient Privacy & HIPAA. Available: www.syndromic.org/pdf/con2-PG-7b.pdf. (Question 3: "Syndrome reporting is not mandated like disease reporting: yes/no/other.")

[21] Drociuk, D., & Gibson, J. (2003). Experience of Syndromic Surveillance Systems with Issues of Patient Privacy & HIPAA. Available: www.syndromic.org/pdf/con2-PG-7b.pdf. (Question 9: "Concerns about adequate data security?")

Dan Drociuk, Director, Bioterrorism Surveillance and Response Program, South Carolina Department of Health and Environmental Control. Contributor to HIPAA Task Team Call, March 19, 2004.

A. Richard Melton, DrPH, Deputy Director, Utah Department of Health. Presenter on HIPAA Task Team Call, March 19, 2004.

Richard Platt, MD, Professor, Harvard Medical School. Contributor to HIPAA Task Team Call, March 19, 2004.

Robert T. Rolfs, MD, MPH, State Epidemiologist, Utah Department of Health. Contributor to HIPAA Task Team Call, March 19, 2004.

Robin Ikeda, MD, MPH, Associate Director of Science in the Epidemiology Program Office, CDC. Personal Communication March 19, 2004.

Beverly Dozier, JD, Privacy Rule Coordinator, CDC. Personal Communication March 19, 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 March 19, 2004.

References

CDC website, Division of Public Health Surveillance and Informatics (2002). Syndromic Surveillance: An applied approach to outbreak detection [On-line]. Available: www.cdc.gov/epo/dphsi/syndromic.htm.

CDC's Focus Area B covers "Surveillance and Epidemiology Capacity"; www.bt.cdc.gov/planning/continuationguidance/pdf/guidance_intro.pdf

CSTE website (2002). Public Health Surveillance for the 2002 Olympic Winter Games [On-line]. Available: www.cste.org.

Detection of Public Health Emergencies Act, Utah. Stat. Ann. 26-12B-101 (2003).

Drociuk, D., & Gibson, J. (2003). Experience of Syndromic Surveillance Systems with Issues of Patient Privacy & HIPAA. Available: www.syndromic.org/pdf/con2-PG-7b.pdf.

Gesteland, Per H. Legal Perspectives of Implementing Syndromic Surveillance Systems-Utah Case Study . Available: www.syndromic.org/pdf/con2-PG-7b.pdf.

Gesteland, Per H., et al (2002). Rapid Deployment of an Electronic Disease Surveillance System in the State of Utah for the 2002 Olympic Winter Games [On-line]. Available: www.health.pitt.edu/rods/LIBRARY/Per.Gesteland.AMIA.2002.Final.pdf

Mostashari F, Hartman J. *Syndromic surveillance: A local perspective*. J. Urban Health. 2003 Jun; 80 (2Suppl 1): i 1-7.

Platt, Richard., et al. *Syndromic Surveillance Using Minimum Transfer of Identifiable Data: The Example of the National Bioterrorism Syndromic Surveillance Demonstration Project*. J. Urban Health. 2003 Jun; 80 (2 Suppl 1) 25i-31i.

Online Resources

Federal Government Resources

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

Center for Disease Control and Prevention- Division of Public Health Surveillance and Informatics www.cdc.gov/epo/dphsi/syndromic.htmcs

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

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

Utah http://health.utah.gov/

South Carolina www.scdhec.net/

Associations, Nonprofit Organizations, and Academic Institutions

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

Other

RODS Laboratory www.health.pitt.edu/rods/

Syndromic.org www.syndromic.org

Utah Olympics www.utah.com/olympics/

Association of State and
Territorial Health Officials

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