Homeland Security and HIM

Save to myBoK

This practice brief has been updated. See the latest version here. This version is made available for historical purposes only.

Following the terrorist attacks in New York City, Pennsylvania, and Washington, DC, on September 11, 2001, the United States Congress enacted the Patriot Act in 2001 and the Homeland Security Act in 2002. The passage of these two acts, followed by the implementation of the Health Insurance Portability and Accountability Act (HIPAA) privacy rule on April 14, 2003, has led to confusion for caregivers and HIM professionals as to how to respond to requests from public health departments and others for protected health information (PHI) using the phrase "homeland security." This practice brief provides a brief analysis of the Homeland Security and Patriot Acts, background about mandatory reporting of health information, and an overview of syndromic reporting, the newest form of mandatory reporting. In addition, this article includes practical facts to help you respond to requests for PHI.

Homeland Security Act

The primary mission of the Homeland Security Act is to prevent terrorist attacks within the US, reduce the vulnerability of the United States to terrorism, and minimize damage and assist in recovery for terrorist attacks that occur in the United States.[1,2]

This act provides the secretary of Homeland Security with the authority to direct and control investigations that require access to information needed to investigate and prevent terrorism.[3] This authority can be interpreted to include requests for PHI of any type without the expressed authorization of the patient or legal guardian. The Homeland Security Act further states that PHI is protected from unauthorized disclosure and is to be handled and used only for the performance of official duties.[4] Therefore, redisclosure would be restricted to those who need to know the information in order to perform their job. This is compatible with the HIPAA privacy rule.

Patriot Act

The major objective of the Patriot Act is to deter and punish terrorist acts in the United States and around the world and to enhance law enforcement investigations.[5] The Patriot Act allows for the emergency disclosure of electronic communications to protect life. Under the Foreign Intelligence Surveillance Act, the Patriot Act allows the director of the Federal Bureau of Investigation or a designee of the director to apply for an order requiring the "production of any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities."[6]

The required production of these tangible things may include PHI protected under HIPAA. However, procedural safeguards outlined in the section must be followed. Each application for a production order must be made to a judge or magistrate, and the judge must demonstrate that the records concerned are sought for an authorized investigation not concerning an American or to protect against terrorism or clandestine intelligence.[7]

Section 223 provides civil liability for certain unauthorized disclosures to protect the private information gathered by the government.[8] Any willful disclosure of a record obtained in an investigation by a law enforcement officer or a government entity that is not a proper disclosure in the performance of the official functions constitutes a violation.

The act should provide some comfort to privacy officers because it states, "A person who, in good faith, produces tangible things under an order pursuant to this section shall not be liable to any other person for such production, such production shall not be deemed to constitute a waiver of any privilege in any other proceeding or context."[9]

Comparing the Homeland Security and Patriot Acts with HIPAA

In reviewing these acts and comparing them with HIPAA, it can be determined that all three concur that records are an organization's or agency's greatest asset. Both the Homeland Security and Patriot Acts are legislation passed into law by Congress in order to protect the citizens of the United States and the nation at large from any potential or viable threat.

In order to understand these acts and their basic intent, health information professionals and their colleagues must recognize that the US government is permitted to access any and all information it deems necessary in order to protect the nation. It is a good faith effort that PHI is released to the requesting authority without delay, provided that the appropriate identification of the government official is obtained and verified (a copy of identification, an office location, and the particular branch of government requesting the information). HIPAA regulations currently permit these disclosures and require that they be recorded in the accounting of disclosures. A patient or legal guardian's authorization is not required when a request is made on behalf of either the Homeland Security or Patriot Acts.

Public Health Surveillance

The duty to report certain health information already exists in the United States, found in various federal and state statutes. Healthcare facilities and providers must report births and deaths, treatment of gunshot wounds, suspicion of child and elder abuse, industrial accidents, as well as cancer cases and communicable and other diseases. This is referred to as mandatory reporting. Historically, the primary purpose of mandatory reporting has been to provide public health officials with the necessary information to protect the public's health by tracking communicable diseases and other conditions.

Syndromic Surveillance in Bioterrorism and Outbreak Detection

The recent events related to bioterrorism and the sudden emergence of outbreaks of West Nile virus, monkeypox, anthrax, and severe acute respiratory syndrome (SARS) have prompted health agencies to seek additional methods of disease surveillance. The most common method used to acquire additional health information is called syndromic surveillance. Its main purpose, according to the Division of Public Health Surveillance and Informatics from the Centers for Disease Control and Prevention (CDC), is to monitor "nonspecific clinical information that may indicate a bioterrorism-associated disease before a specific diagnosis is made."[10]

The main factors influencing further development of new syndromic surveillance systems are the emerging threat of bioterrorism and the growing availability of electronic health data. The CDC provides information and guidance to public health practitioners and healthcare agencies interested in implementing syndromic surveillance systems.[11]

What makes syndromic surveillance unique from other systems is the indicator data types used to collect health information. The data types used in syndromic systems include "events preceding clinical diagnosis: test requests, emergency room chief complaints, clinical impressions on ambulance run sheets, prescriptions filled, retail drug and product purchases, school or work absenteeism, and constellations of medical signs and symptoms in people seen in various clinical settings."[12]

Balancing the Right to Privacy with Protecting the Public

Although the public and the healthcare community are concerned about public health authorities having access to a patient's medical record, in most cases the health information used in syndromic systems is de-identified when transmitted to an outside source. The collection of health data is intended to collect clusters of cases, not individual cases.

Whether a fine line or an abyss exists between respecting the privacy of people's health information and protecting the public from bioterrorism depends on perspective. When contrasting the Homeland Security and Patriot Acts with the intent of HIPAA's privacy and security rules, the challenges to public health departments become evident. One fundamental challenge for many healthcare organizations is deciding whether the gap between personal privacy and national security is small or large and how it can be bridged.

Several initiatives show promise for surveillance on the national level while remaining considerate of individual privacy. Public health officials have historically leveraged surveillance systems to identify outbreaks and monitor disease activity among communities. The challenges associated with implementing broader surveillance systems include inadequate infrastructure, data integration barriers due to lack of standards, deficient understanding of public health informatics, and funding.[13]

Some resistance to a national syndromic surveillance system could arise from groups already heavily invested in developing alternate solutions. Many states and counties have already committed significant time and resources to developing surveillance systems that serve citizens within their boundaries. This independent activity has generated many impressive public health surveillance systems, albeit in a somewhat federated fashion. However, these federated surveillance systems often cannot share data due to a lack of standards. The resulting data-sharing roadblocks are found at all levels of technology and consist of incompatible hardware, software versions that do not talk to each other, and inconsistent data definitions to name a few.

Data quality presents another challenge in implementing public health surveillance. In many instances in healthcare facilities, a nonclinician may enter the admitting diagnosis prior to the patient being assessed by a licensed independent practitioner, and the clinical relevance of the data may be questionable. Data inaccuracy in syndromic surveillance systems becomes an obstacle to wholesale adoption of such systems if user comfort levels with the quality of the data are not satisfactory.

Public health information systems can deliver valuable information for national security efforts without compromising patient privacy. While the nation's capacity to respond to bioterrorism may depend on further development of surveillance systems, there are many diverse efforts trying to balance individual privacy with protection of the public health. Syndromic surveillance systems will likely evolve as obstacles are overcome, standards are created, and the public accepts and supports the cost of adopting such a system.

HIM Roles: Suggestions for the Workplace

HIM professionals must expand their knowledge to include mandatory reporting under the Patriot and Homeland Security Acts. In addition, they must become well acquainted with the members of their organizations who are responsible for the required mandatory reporting and work collaboratively in order to effectively identify, obtain, and release information to the appropriate authorities. No single department can work alone in this area, since the information that is obtained occurs during registration (specific demographics), during the course of treatment (clustering of signs and symptoms that could potentially cause a threat to the public at large), and at the time of discharge (identifying key diagnoses).

HIM professionals should consider taking the following actions:

- Develop a matrix demonstrating all of the various reporting requirements (e.g., codes that are required to be submitted).
- Determine whether the identified needs can be met through the HIM abstracting system. If not, contact the technology department to develop an automatic reporting method or work with the department responsible for this required reporting.
- Determine if this information needs to be reported through the accounting of disclosures and react accordingly.
- Take the initiative to serve on the team establishing the initial policies for their facility's syndromic surveillance.

Suggestions for Component State Associations

Component state associations (CSAs) should take a strong role in shaping the development of public health systems for required reporting. The infancy of both the Patriot and Homeland Security Acts offers CSAs the opportunity to work with other associations and agencies (such as the state hospital association, department of health, or long-term care licensing agency) with an interest in reviewing current required reporting rules and integrating new requirements into systems as they are identified.

State hospital associations may be a good place to identify rule makers within the state. In most states, the department of health is given the authority to establish mandatory reporting programs; in some instances, special commissions have been established to monitor this function. Other state agencies that are likely to be involved include departments of health and human services, state bureaus of investigation, and separate registries if established by the state government.

Groups responsible for overseeing or managing reporting systems should welcome HIM's experience in data management and efficient reporting processes, understanding of coded data, and overall grasp of patient privacy and confidentiality. Even with sophisticated electronic reporting systems, information managers are needed to organize information and turn data into knowledge. HIM professionals and CSAs have an opportunity and an obligation to offer and apply their knowledge and abilities to this process.

Strategies Your CSA Can Use to Make a Difference in Rule Making

The strength of a CSA is, of course, found within its membership. Your association will be seen as an important entity when other associations see a representative of your CSA in virtually every healthcare setting, not just hospitals. Methods proven to be effective in dealing with other associations include:

- Make alliance building a major initiative for your CSA. Form a work group that consists of HIM professionals representing all geographic regions of the state and as many different healthcare settings as possible. Identify individuals who have a working knowledge of mandatory reporting or who are willing to learn.
- Do your homework—get educated! Learn as much as you can, individually and as a group, about the rules in your state and the challenges faced by healthcare providers who are responsible for reporting. Identify areas that need improvement and areas that overlap disciplines. Realize that once data is reported, it is available to many entities and will be analyzed for various purposes.
- Contact other allied healthcare associations who are involved (the state chapter of the Association of Practitioners in Infection Control, the state nurses' association, the state chapter of the American Association for Healthcare Quality). Offer to work together to enhance the reporting process and address whatever issues arise as a team.
  Offer educational opportunities for healthcare workers and law enforcement personnel. Build an alliance with the state hospital association and the state medical association. Many physicians may be unaware of the reporting requirements and of the enormous amount of information being reported.
- State hospital associations and state health departments often have oversight committees that monitor reporting processes. Ask if a representative of the CSA can serve as a member of the committee (at least in an ex-officio capacity); stress that the members of your association are the information people and that their involvement is critical to the integrity of reported data.

Career Opportunities with Public Health Agencies

Many state health departments employ HIM professionals to manage the databases created by required reporting and through statewide registries. As healthcare oversight, syndromic surveillance, and public and patient safety issues receive more and more national attention, these opportunities will grow. HIM competencies bring value to the work of these agencies. In the future, competency in areas such as data integration, methods of encryption and de-identification, and data analysis tools and techniques will be necessary to compete for new roles that emerge as a result of oversight and surveillance activities. The future roles and competencies of HIM professionals, as described in AHIMA's report "A Vision of the e-HIM Future" should become the HIM credential holder's guide for career planning and development.[14]

Facts to Remember

- The United States government is permitted to access any and all PHI it deems necessary in order to protect the nation.
- PHI should be released to the requesting authority without delay after appropriate verification.
- Appropriate identification of the government official must be obtained and verified, including copy of identification, office location, and the particular branch of government requesting the information.
- HIPAA regulations currently permit these disclosures.
- These disclosures must be recorded in the accounting of disclosures.
- A patient or legal guardian's authorization is not required when a request is responded to under either the Homeland Security or Patriot Acts.

Mandatory reporting requirements as required by the Homeland Security and Patriot Acts require a total organizational effort. HIM professionals are at the center of this involvement. HIM professionals who are aware of the requirements and limitations of these statutes and regulations can direct and provide the security that their organizations require.

For more information on mandatory reporting in the US and syndromic surveillance systems in bioterrorism and outbreak detection, see Appendix A: Mandatory Reporting–Balancing Patients' Privacy Rights with Public Health Interests and Appendix B: Syndromic Surveillance Systems in Bioterrorism and Outbreak Detection, available in the FORE Library: HIM Body of Knowledge.

Notes

1. "Homeland Security Act of 2002." Public Law 107-296, November 25, 2002. Available online at www.dhs.gov/interweb/assetlibrary/hr_5005_enr.pdf.
2. Ibid., 116 Stat., Section 101.
3. Ibid., 116 Stat., Section 201.
4. Ibid., 116 Stat., Section 221.
5. "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001." Public Law 107-56, October 26, 2001. Available online at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ056.107.pdf.
6. Ibid., 115 Stat. 287.
7. Ibid., 115 Stat. 288(2).
8. Ibid., 115 Stat. 293.
9. Ibid., 115 Stat. 288.
10. Centers for Disease Control and Prevention (CDC), Division of Public Health Surveillance and Informatics (DPHSI). "Syndromic Surveillance: An Applied Approach to Outbreak Detection." Available online at www.cdc.gov/epo/dphsi/syndromic.htm.
11. Centers for Disease Control and Prevention. "Framework for Evaluating Public Health Surveillance Systems for Early Detection of Outbreaks: recommendations from the CDC Working Group." MMWR 2004; 53(No. RR-5): 1-13. Available online at http://www.cdc.gov/mmwr/PDF/rr/rr5305.pdf.
12. Ibid.
13. Public Health Informatics Institute. "Highlights of NACCHO Surveys of Local Public Health Agencies." Available online at www.phii.org/lpha_survey_4.html.
14. AHIMA. "A Vision of the e-HIM Future: A Report from the AHIMA e-HIM Task Force." Available online at www.ahima.org.

References

Agency for Healthcare Research and Quality. "Bioterrorism Preparedness and Response: Use of Information Technologies and Decision Support Systems." Available online at www.ahcpr.gov/clinic/epcsums/bioitsum.pdf.

CDC, DPHSI. "Syndrome Definitions for Diseases Asso-ciated with Critical Bioterrorism-associated Agents." Available online at www.bt.cdc.gov/surveillance/syndromedef/index.asp.

Security Standards Final Rule. 45 CFR Parts 160, 162, 164. *Federal Register* 68, no. 34 (2003). Available online at www.hhs.gov/ocr/hipaa.

"Standards for Privacy of Individually Identifiable Health Information: Final Rule." 45 CFR Parts 160 and 164. *Federal Register* 65, no. 250 (2000). Available online at www.hhs.gov/ocr/hipaa.

Prepared by

Arlene J. Arellano, RHIA
Cynthia Baxter, University of Washington HIA student
Deborah C. Beezley, RHIT
Cindy M. Boester, MS, RHIA
Julie Coleman, RHIA
John Eckmann, MPH
Mary Frazeur, RHIA
Elisa R. Gorton, RHIA
Marilyn M. Houston, RHIA
Wanda Johnson, RHIT
Leticia I. Parks, University of Washington HIA graduate
Carol Ann Quinsey, RHIA, CHPS
Jennifer Pritzker Sender, JD, MPH
Stacie Smith, RHIA
Mary Ann Spott, MPA, MSIS, RHIA, CPHQ, CPUR

Cathy Stevens, RHIT
Sakiko Taguchi, University of Washington HIA student

Article citation:
AHIMA Homeland Security Work Group. "Homeland Security and HIM." (AHIMA Practice Brief) *Journal of AHIMA* 75, no.6 (June 2004): 56A-D.