Homeland Security Act, Patriot Act, Freedom of Information Act, and HIM - Retired

Save to myBoK

Editor's note: This update replaces the June 2004 practice brief "Homeland Security Act and HIM."

After 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 HIPAA privacy rule on April 14, 2003, led to confusion for caregivers and HIM professionals as to how to respond to requests for protected health information (PHI) that use the phrase "homeland security" from public health departments, law enforcement agencies, federal agencies, and others.

This practice brief provides a brief analysis of the Homeland Security Act, Patriot Act, and Freedom of Information Act; 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 United States, 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] The Homeland Security 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 express authorization of the patient or legal guardian. It 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 to perform their jobs, which is compatible with the HIPAA privacy rule.

The Homeland Security Act also established the US Department of Homeland Security. The Department of Homeland Security includes many other organizations, such as the Federal Emergency Management Agency, US Coast Guard, US Secret Service, and Transportation Security Administration.

The Department of Homeland Security boasts the first statutorily required privacy office within a federal agency. Mary Ellen Callahan was appointed the chief privacy officer and chief FOIA officer in March 2009. The privacy office is primarily responsible for evaluating privacy's effect on the department's programs, systems, and initiatives. It is further required to mitigate any anticipated effect on privacy.

The privacy office's objectives include:

- Evaluating the department's legislative and regulatory proposals that involve the collection, use, and disclosure of personally identifiable information
- Centralizing and providing program oversight and implementing all FOIA and Privacy Act operations
- Operating a privacy incident response program that addresses incidents involving personally identifiable information
- Responding to, investigating, and addressing complaints of privacy violations
- Providing training, education, and outreach that build the foundation for privacy practices across the department and create transparency[5]

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 investigatory tools"[6] by dramatically reducing restrictions pertaining to law enforcement requests to search telephone records, e-mail communication, and health records. The Patriot Act allows for the emergency disclosure of electronic communications to protect life and broadens the definition of terrorism to include acts of domestic terrorism. 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."[7]

The required production of these tangible things may include PHI protected under HIPAA. 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.[8]

Section 223 provides civil liability for certain unauthorized disclosures to protect the private information gathered by the government.[9] 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 Patriot 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."[10]

In March 2010, after months of debate, Congress voted to extend three expiring provisions of the Patriot Act for one full year. The provisions set to expire pertain to business records, roving wiretaps, and so-called "lone-wolf" investigations and continue to provide law enforcement agencies with broad discretion when gathering information.

Freedom of Information Act

The Freedom of Information Act (FOIA), as currently amended, represents the first implementation of information freedom legislation in the United States. Originally signed into law by President Lyndon B. Johnson in 1966, FOIA provides for the partial or full disclosure of unreleased information and documents controlled by the US government. It further defines all records subject to disclosure, outlines procedures, and identifies exemptions to the statute.

FOIA exemptions address sensitivity and personal rights, including:

1. "Those documents properly classified as secret in the interest of national defense or foreign policy;
2. Related solely to internal personnel rules and practices;
3. Specifically exempted by other statutes;
4. A trade secret or privileged or confidential commercial or financial information obtained from a person;
5. A privileged interagency or intraagency memorandum or letter;
6. A personnel, medical, or similar file the release of which would constitute a clearly unwarranted invasion of personal privacy;
7. Compiled for law enforcement purposes, the release of which

    a. could reasonably be expected to interfere with law enforcement proceedings,
    b. would deprive a person of a right to a fair trial or an impartial adjudication,
    c. could reasonably be expected to constitute an unwarranted invasion of personal privacy,
    d. could reasonably be expected to disclose the identity of a confidential source,
    e. would disclose techniques, procedures, or guidelines for investigations or prosecutions, or
    f. could reasonably be expected to endanger an individual's life or physical safety;

8. Contained in or related to examination, operating, or condition reports about financial institutions that the SEC regulates or supervises; or
9. And those documents containing exempt information about gas or oil wells."[11]

In 1974, Congress voted to override President Gerald R. Ford's veto of the Privacy Act Amendments. The Privacy Act provides protection of records that can be retrieved by personal identifiers such as name or Social Security number. Individuals are entitled access to records and to request correction of these records. The act prohibits disclosure of these records without appropriate written consent of the individual to whom the records pertain, unless one of the 12 disclosure exceptions within the Privacy Act applies. The Privacy Act applies to federal agencies only and includes only records within the possession of those agencies.

These amendments further define the rights of individuals requesting government records and strengthened privacy efforts. From 1986 to 2001, FOIA had several amendments that provided agencies with the ability to withhold information from the public. All of these restrictions were revoked in January 2009 by President Barack Obama in an effort to encourage transparency in government records.

FOIA was further addressed in 1996 when the Electronic FOIA, or E-FOIA, required all agencies to make certain records available electronically and provide electronic access for citizens who request it.

FOIA, the Privacy Act of 1974, and all subsequent amendments are consistent with the HIPAA privacy rule.

Comparison with HIPAA

In reviewing these acts and comparing them with HIPAA, all four concur that records are an organization's or agency's greatest asset. The Homeland Security Act, Patriot Act, and FOIA are legislation passed into law by Congress to protect the citizens of the United States and the nation at large from any potential or viable threat.

To understand these acts and their basic intent, HIM professionals and their colleagues must recognize that the US government is permitted to access any and all information it deems necessary to protect the nation. PHI should be released to the requesting authority without delay, provided that the appropriate identification (a copy of identification, an office location, and the particular branch of government requesting the information) of the government official is obtained and verified. HIPAA regulations currently permit these disclosures without a patient's or legal guardian's authorization and require that they be recorded in the accounting of disclosures. These types of disclosures could be listed as examples in an organization's notice of privacy practice.

Public Health Surveillance

The duty to report certain health information already exists in the United States and is 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, and industrial accidents, as well as cancer cases and communicable and other diseases. This duty 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

Events related to bioterrorism and the sudden emergence of outbreaks of H1N1 influenza, avian flu, West Nile virus, anthrax, and severe acute respiratory syndrome 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 at the Centers for Disease Control and Prevention, is to monitor "nonspecific clinical information that may indicate a bioterrorism-associated disease before a specific diagnosis is made."[12]

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 Centers for Disease Control and Prevention provides information and guidance to public health practitioners and healthcare agencies interested in implementing syndromic surveillance systems.[13]

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 that might precede a clinical diagnosis (e.g., patient's chief complaints in emergency departments, clinical impressions on ambulance log sheets, prescriptions filled, retail drug and product purchases, school or work absenteeism, and constellations of medical signs and symptoms in persons seen in various clinical settings)."[14]

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 deidentified 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 individual health information and protecting the public from bioterrorism depends on perspective. In contrasting the Homeland Security Act, Patriot Act, and FOIA 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.[15]

Some resistance to a national syndromic surveillance system could arise from groups already heavily invested in developing alternate solutions. Many states and counties already have 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 because of 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 before the patient is 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. Although 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 likely will 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 be knowledgeable about mandatory reporting under the Homeland Security Act, Patriot Act, and FOIA. In addition, they should know which members of their organizations are responsible for mandatory reporting and work collaboratively 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:

- 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. These acts offer CSA leaders the opportunity to work with other associations and agencies (such as a state hospital association, department of health, or long-term care licensing agency) with an interest in reviewing 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.

The HIM professional's knowledge of data management, reporting processes, coded data, and patient privacy and confidentiality requirements provide a needed resource to state agencies. Even with sophisticated electronic reporting systems, information managers are needed to organize information and turn data into knowledge. HIM professionals and CSAs have 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 its members. Your CSA will be perceived as an important entity when other CSAs see one of your representatives in virtually every healthcare setting, not just hospitals. Methods proven to be effective in dealing with other CSAs include:

- Making 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 are reported, they are available to many entities and will be analyzed for various purposes.
- Contact other allied healthcare associations that are involved (e.g., the state chapter of the Association for Professionals in Infection Control and Epidemiology, the state nurses' association, the state chapter of the American Health Quality Association). Offer to work together as a team to enhance the reporting process and address whatever issues arise. 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.
- Ask if a representative if the CSA can serve as a member (at least in an ex officio capacity) of an oversight committee that monitors reporting processes for a state hospital association or state health department. Stress that the members of your CSA 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 due to required reporting and 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 deidentification, and data analysis tools and techniques will be necessary to compete for new roles that emerge as a result of oversight and surveillance activities.

Facts to Remember

- The United States government is permitted to access any and all PHI it deems necessary 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 a 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 the Patriot Act.

For more information on mandatory reporting in the United States and syndromic surveillance systems in bioterrorism and outbreak detection, see "Mandatory Reporting--Balancing Patients' Privacy Rights with Public Health Interests"[16] and "Syndromic Surveillance Systems in Bioterrorism and Outbreak Detection,"[17] available online in the AHIMA Body of Knowledge at www.ahima.org.

Notes

1. "Homeland Security Act of 2002." Public Law 107-296, November 25, 2002.Available online at www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf.
2. Ibid., 116 Stat., Section 101.
3. Ibid., 116 Stat., Section 201.
4. Ibid., 116 Stat., Section 221.
5. U.S. Department of Homeland Security. "About the Privacy Office" Accessed online November 2010 at http://www.dhs.gov/xabout/structure/editorial_0510.shtm
6. "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.
7. Ibid., 115 Stat. 287.
8. Ibid., 115 Stat. 288(2).
9. Ibid., 115 Stat. 223.
10. Ibid., 115 Stat. 288
11. US Securities and Exchange Commission. "Freedom of Information Act Exemptions." Available online at www.sec.gov/foia/nfoia.htm.
12. Centers for Disease Control and Prevention, Division of Public Health Surveillance and Informatics. "Syndromic Surveillance: An Applied Approach to Outbreak Detection." Available online at www.cdc.gov/ncphi/disss/nndss/syndromic.htm.
13. Buehler, James W., Richard S. Hopkins, J. Marc Overhage, et al.. "Framework for Evaluating Public Health Surveillance Systems for Early Detection of Outbreaks: Recommendations from the CDC Working Group." *MMWR Recomm Rep.* 2004;53(RR-5):1?11. Available online at www.cdc.gov/mmwr/PDF/rr/rr5305.pdf.
14. Ibid.
15. Public Health Informatics Institute. "Highlights of NACCHO Surveys of Local Public Health Agencies." Available online at www.phii.org/lpha_survey_4.html.
16. Baxter, Cynthia, and Sakiko Taguchi. "Homeland Security and HIM. Appendix A: Mandatory Reporting?Balancing Patients' Privacy Rights with Public Health Interests" *Journal of AHIMA* 75, no.6 (June 2004): web extra.
17. Parks, Leticia I. "Homeland Security and HIM. Appendix B: Syndromic Surveillance Systems in Bioterrorism and Outbreak Detection" *Journal of AHIMA* 75, no.6 (June 2004): web extra.

References

Agency for Healthcare Research and Quality. "Bioterrorism Preparedness and Response: Use of Information Technologies and Decision Support Systems." Available online at http://archive.ahrq.gov/clinic/tp/bioittp.htm.

Centers for Disease Control and Prevention, Division of Public Health Surveillance and Informatics. "Syndrome Definitions for Diseases Associated with Critical Bioterrorism-associated Agents." Available online at www.bt.cdc.gov/surveillance/syndromedef/index.asp.

Department of Health and Human Services, "Health Insurance Reform; Security Standards Final Rule." 45 CFR Parts 160, 162, 164, *Federal Register* 68, no. 34 (2003). Available online at http://aspe.hhs.gov/admnsimp/final/fr03-8334.pdf.

Department of Homeland Security. Available online at www.dhs.gov/index.shtm.

Department of Homeland Security, Privacy Office. Available online at www.dhs.gov/xabout/structure/editorial_0338.shtm.

"Freedom of Information Act." (5 U.S.C. § 552, As Amended By Public Law No. 104-231, 110 Stat. 3048). Available online at www.justice.gov/oip/foia_updates/Vol_XVII_4/page2.htm.

"Homeland Security Act of 2002." Public Law 107-296. Available online at www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf.

"Patriot Act." Public Law 107-56. Available online at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ056.107.pdf..

"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 http://aspe.hhs.gov/admnsimp/final/pvcguide1.htm.

Prepared by

Lou Ann Wiedemann, MS, RHIA, FAHIMA, CPEHR

Prepared by (original)

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, RHIA
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, RHIA

Article citation:
AHIMA. "Homeland Security Act, Patriot Act, Freedom of Information Act, and HIM - Retired." (Updated November 2010).
