Changing Face of Public Health Reporting

Save to myBoK

by Michelle Dougherty, RHIA

In recent months, anthrax outbreaks and concern over bioterrorism threats have created a greater need for the US to have a system to monitor and report public health information in a timely manner. The Centers for Disease Control and Prevention (CDC) are developing standards for a new approach to addressing the shortcomings in the current reporting system. In doing so, it will tackle the critical issues of consistency, timeliness, and security of public health data.

While the public health sector is revamping its systems for reporting, providers are tackling the HIPAA privacy rule and evaluating how protected health information is used and disclosed in their organizations. This article will focus on upcoming changes to public health reporting that will have an impact on many healthcare organizations. It will also provide an understanding of the principles and terminology to help HIM professionals ask the right questions when it comes to public health reporting.

A Risky System

In the current communication process, information typically flows from the provider setting to the local or state department of health. The department of health then eliminates demographic information and submits it to the CDC. It can take days, weeks, or months before information is received, making active surveillance of public health outbreaks or threats impossible.

Additionally, there is inconsistency in the data definitions and format of information submitted across the country. Information can be submitted in paper form, on diskette, or electronically through various types of connections. At the health department level, there are various databases to report information to the CDC, which often results in duplicate data entry into multiple stand-alone systems and databases.

Another concern with the current system is the lack of uniform confidentiality and security standards as information is transferred from the local or state level to the CDC. Although the information is stripped of demographic and case record information, there is still a risk as information flows in a variety of non-secure formats and connections to the CDC.

A System of Prevention

To address these issues and improve the function of national disease surveillance in the US, the CDC is implementing the National Electronic Disease Surveillance System (NEDSS). The goal of NEDSS is to streamline the flow of information between the provider setting and the public health agencies. For a provider, there should be a reduction in the time it takes to fill out paperwork or complete data entry. One of the goals of NEDSS is to have lab systems automatically report pertinent lab results in "real time." As a lab test is conducted and results are finalized, information would automatically be transmitted directly to the state or local department of health, reducing the time delay between the provider and health department and allowing for timely and active surveillance of potential public health threats when necessary.

This major shift in reporting, particularly to a system that automatically discloses highly confidential information, raises a number of red flags. Is patient privacy protected? Will the transmission be secure? One of the primary drivers for NEDSS was to address confidentiality and security issues. Until now, states had been free to set up their own systems with varying formats, levels of security, and confidentiality policies. The CDC is addressing this issue by establishing confidentiality and security protocols and standards.

For data transmission, the Internet will be used as a backbone for communication, but transmission will be conducted through a secure data network (SDN). The SDN acts as a secure pipeline through the Internet in which data files are encrypted and transferred from the health department to the CDC. Another security measure will be the use of digital certificates to authenticate the source and integrity of the data submitted. Overall, the new standards in NEDSS will raise the bar for security in public health reporting.

How HIPAA Fits In

Fully understanding how information is reported to public health agencies is an important step in tackling HIPAA preparedness. Pinpointing how and where mandatory public health data is disclosed in your organization will be critical. Public health reporting comes into play in at least three sections of the HIPAA privacy rule:

- Use and disclosure of protected health information for public health activities is acceptable under HIPAA (section 164.512[b]). An individual is not required to sign a consent or authorization, nor does the individual have the ability to agree or object.
- If public health data is disclosed, the Notice of Privacy Practices must include the fact that protected health information will be disclosed for public health activities without the individual's written consent or authorization (164.520[b]iiB).
- If information is disclosed for public health purposes, there must be a mechanism to track the disclosures in case an individual requests an accounting of disclosures (164.528[b]).

Public health reporting falls outside the definition of treatment, payment, and healthcare operations and also falls outside the other exceptions to the accounting of disclosures requirement. As a result, disclosures made for public health purposes should be tracked to ensure that a record of disclosures can be provided to an individual upon his or her request.

A Continuing Process

Understanding how and where information is reported for public health purposes will assist in collecting information for an accounting of disclosures. As the communication process changes and becomes more automated, a mechanism is needed to identify which individuals had information reported and when, the name of the entity receiving the information, the type of information disclosed, and the purpose for the disclosure of the information.

The concept for changes in the way public health information is reported began in 1995 with the CDC's report "Integrating Public Health Information and Surveillance Systems." Since then a number of states have started to upgrade their information systems and standards, but there are varying degrees of readiness. As you prepare for HIPAA, determine how information is collected and reported now and changes that are expected as the public health reporting system is revamped.

Shape the Electronic Health Record

Participate in a FORE-sponsored study, "Standards for the Content of Electronic Health Records," via a Web-based survey. The focus of the research, conducted by Valerie J.M. Watzlaf, PhD, RHIA, is to identify usage of aspects of the ASTM standards on electronic health record content and determine how these standards meet users' needs. To participate, e-mail valgeo@pitt.edu or call (412) 383-6647 or (412) 383-6650.

References

"Integrating Public Health Information and Surveillance Systems: A Report and Recommendations." Centers for Disease Control and Prevention, 1995. Available online at www.cdc.gov/od/hissb/docs/katz.htm.

Koplan, Jeffrey P. "Building Infrastructure to Protect the Public's Health." Public Health Training Network Broadcast, September 21, 2001. Available online at www.phppo.cdc.gov/documents/koplanASTHO.pdf

"Standards for Privacy of Individually Identifiable Health Information; Final Rule." 45 CFR Parts 160 and 164. Federal Register 65, no. 250 (December 28, 2000). Available at http://aspe.hhs.gov/admnsimp/.

"Supporting Public Health Surveillance through the National Electronic Disease Surveillance System (NEDSS)." Centers for Disease Control and Prevention. Available at http://www.cdc.gov/od/hissb/docs.htm.

Michelle Dougherty (*michelle.dougherty@ahima.org*) *is an HIM practice manager at AHIMA.*

Article citation:

Dougherty, Michelle. "The Changing Face of Public Health Reporting." *Journal of AHIMA* 73, no.4 (2002): 61-2.

Driving the Power of Knowledge