Data Stewardship: Global Recommendations for Local Action

by Crystal Kallem, RHIT

Healthcare's expanded use of technology and increasing ability to disperse information with the push of a button requires that organizations pay special attention to data stewardship at the local level. HIM professionals influence how data are managed and dispersed, and thus they have a duty to promote appropriate healthcare data stewardship principles.

This article outlines recommendations from the National Committee on Vital and Health Statistics (NCVHS) for the appropriate use of data across the healthcare continuum.

Importance of Data Stewardship

The American Medical Informatics Association defines data stewardship as the "responsibilities and accountabilities associated with managing, collecting, viewing, storing, sharing, disclosing, or otherwise making use of personal health information."[1] It further states that "principles of data stewardship apply to all the personnel, systems, and processes engaging in health information storage and exchange within and across organizations."

AHIMA's practice brief "Health Data Access, Use, and Control" calls out the importance of data stewardship, stating "we should approach the application of stewardship first by recognizing that healthcare is becoming increasingly patient-centered, and we must put patients at the center of the decision we make about their health informations."[2]

Appropriate data stewardship is a key to building transparency and trust throughout all organizations that use health data.

When data are properly maintained, the benefits of their expanded use include:

- Enhanced access to information
- Patient safety alerts at the point of care
- Health maintenance reminders
- Readily accessible information in an emergency
- Complete information for coordination of care among providers
- Automated, structured data collection
- Efficient access to more comprehensive data
- Potential identification of new opportunities for improvement in care delivery
- Access to more complete and timely data to support clinical and population research and disease prevention and control

However, potential for harm is equally apparent in the improper management of data. This includes:

- Potential erosion of consumer trust
- Failure of consumers to seek treatment or share full personal information because they do not understand or trust how their data might be used or how their identity is protected
- Risk for discrimination, personal embarrassment, and group-based harm
- Greater ability to re-identify data that has been de-identified and share data through health information exchange networks

NCVHS Framework for Data Uses

In 2007 the Office of the National Coordinator for Health Information Technology asked NCVHS to develop a conceptual framework to balance the benefits, sensitivities, obligations, and protections of secondary uses of health data.

As a result of testimony from industry experts, NCVHS proposed a set of recommendations "intended to provide a framework, for all uses of health data, irrespective of whether the data is protected health information collected and used by a HIPAA covered entity or business associate, or personal health information collected and used by an organization that is not a HIPAA covered entity."[3]

NCVHS calls for a transformation in which focus is placed on appropriate data stewardship for all uses of health data by all users, regardless of whether an organization is covered under HIPAA. Its recommendations define attributes for data stewardship that include, but are not limited to, the following.

Accountability and chain of trust within HIPAA. NCVHS recommends that covered entities be specific in their business associate contracts about:

- What identifiable health data may be used and for what purpose, by both the business associate and its agents
- What HIPAA de-identified data may be used and to whom they are supplied
- The requirement that business associates have contracts with their agents that are equivalent to business associate contracts
- Use of the HIPAA definition for any de-identification of protected health information

NCVHS also calls for the Department of Health and Human Services (HHS) to issue guidance that any organization that provides data transmission of protected health information and requires access on a routine basis to the protected health information, such as a health information exchange or e-prescribing gateway, is a business associate.

Transparency. NCVHS urges HHS to issue guidance to ensure that individuals are informed about all potential uses of their health data through education and clarity in the notice of privacy practices and other HIPAA documentation, as well as making information available about specific uses and users of protected health information when requested. NCVHS recommends that HHS develop and maintain a multifaceted national education initiative that would enhance transparency regarding uses of health data in an understandable and culturally sensitive manner.

Individual participation and control over personal health information. NCVHS calls for HHS to urge the Federal Trade Commission to use its full authority over organizations that collect personal health information but are not covered entities or business associates under HIPAA. This recommendation aims to ensure that Web sites collecting personal health information maintain privacy policies that fully inform users of how their information will be used. It would also help prevent organizations from engaging in misleading advertising or other deceptive practices.

De-identification of health data. NCVHS recommends that HHS issue guidance to covered entities that the HIPAA definition of de-identification be the only permitted means to de-identify protected health information. NCVHS also indicates that significant concerns regarding uses of de-identified data were raised during testimony that warrant additional investigation. As a result, NCVHS will conduct hearings to make subsequent recommendations on this topic in the future.

Security safeguards and controls. NCVHS calls for HHS to issue guidance to covered entities to promote the use of technical security measures to reduce unauthorized access and ensure that business associates and agents are fully compliant with the HIPAA security rule requirements for authorization, access, authentication, and audit control. NCVHS further recommends that this guidance should also be directed to organizations that are not covered entities that maintain or transmit personal health information.

Data quality and integrity measures. NCVHS recommends that HHS issue guidance to address the precision, accuracy, reliability, completeness, and meaning of data used for quality measurement, reporting, and improvement as well as other uses of health data.

Oversight of data uses. NCVHS notes that quality measurement, reporting, and improvement remain within the scope of healthcare operations when conducted by covered entities, their business associates, and their agents; across covered entities within an organized healthcare arrangement; and when under the accountability and data stewardship principles inherent in HIPAA. However, NCVHS states that these uses may benefit from a voluntary, proactive oversight process accountable to senior management and governance of the institution to ensure there is compliance with HIPAA.

NCVHS heard testimony that there is variation in interpretations in regulations addressing human research protections. Additional gaps and clarification in the research definition were also identified. As a result, NCVHS calls for HHS to encourage the Office for Human Research Protections (OHRP) to work collaboratively with the Office for Civil Rights when compiling clarification on the elements contained in the definition of research and to leverage emerging industry tools to aid in distinguishing how requirements apply to uses of health data for quality and research.

Furthermore, HHS was asked to encourage OHRP to widely disseminate its clarifying work beyond the research community to ensure providers, payers, and others who are engaged in quality initiatives receive clarification on when these activities could fall within the scope of research on human subjects. NCVHS will lead efforts, in collaboration with OHRP and other agencies, to further study these areas and make recommendations as appropriate.

The report also offers high-level recommendations for national health information network trial implementations and additional privacy protections addressing needed legislation that expands the definition of covered entities under HIPAA.

Applying Data Stewardship Principles

NCVHS also developed the "Data Stewardship Conceptual Framework for Health Data Uses," which outlines how an organization might approach the complex task of evaluating intended uses of health data. The framework builds upon several industry sources: the "Secondary Uses and Re-Uses of Healthcare Data: Taxonomy for Policy Formulation and Planning" from the American Medical Informatics Association; the "Connecting for Health Common Framework Privacy Principles" from the Markle Foundation; and the National Cancer Institute's Cancer Biomedical Informatics Grid "Framework for Data Sharing Terms and Conditions."

Although no single tool or report can identify all uses and users of health data, nor anticipate all potential new uses or users, the model provides the structure for assessing the complex issues and defining possible courses of action. A sample of the framework appears on below.

Data Stewardship Conceptual Framework for Uses of Health Data

Health Data User and Use Profile
User: Provider, Payer, Clearinghouse, Business Associate or Agent, Federally-sponsored Researcher, Commercial Researcher, Public Health, PHR Vendor, Other
Regulatory status: HIPAA Privacy and Security Rules, State Data Statutes, Common Rule, FDA Research Regulations. VA Research Regulations, HIPAA Privacy Board, Other State Laws, FTC, Other
Identity status: Identifiable, HIPAA De-identified (Safe Harbor), HIPAA De-identified (Statistical), Limited Data Set, Anonymization, Pseudonymization, Other
Analysis of Benefits and Potential Risks
Intended Use of Data: Treatment, Payment, Healthcare Operations, Research, Public Health, Other
Impact: Benefits to Individual and Society, Potential Risk for Harm

Data Stewardship Attributes						
Accountability/Chain of Trust	Transparency	Individual Participation	HIPAA De-identification	Security Safeguards and Controls	Data Quality and Integrity	Oversight of Data Uses

This model from NCVHS aids healthcare organizations in evaluating the need for enhanced data stewardship for any contemplated use of health data.

Source: National Committee on Vital and Health Statistics. "Enhanced Protections for Uses of Health Data: A Stewardship Framework for 'Secondary Uses' of Electronically Collected and Transmitted Health Data." December 2007. Available online at http://ncvhs.hhs.gov/071221lt.pdf.

Notes

1. American Medical Informatics Association. "Toward a National Framework on Secondary Use of Health Data: Testimony to the National Committee on Vital and Health Statistics." July 2007. Available online at www.amia.org/inside/initiatives/healthdata/2007/labkoffbloomrosenncvhssecondarydata.pdf.
2. Burrington-Brown, Jill, Beth Hjort, and Lydia Washington. "Health Data Access, Use, and Control." *Journal of AHIMA* 78, no. 5 (May 2007): 63–66.
3. National Committee on Vital and Health Statistics. "Enhanced Protections for Uses of Health Data: A Stewardship Framework for 'Secondary Uses' of Electronically Collected and Transmitted Health Data." December 2007. Available online at http://ncvhs.hhs.gov/071221lt.pdf.

Resources

AHIMA. "Development of a National Health Data Stewardship Entity: Response to Request for Information." August 3, 2007. Available online at www.ahima.org.

Dimick, Chris. "Health Data's Second Life." *Journal of AHIMA* 78, no. 10 (Nov.–Dec. 2007): 44–48.

Acknowledgments

Beth Hjort, RHIA, CHPS

Allison Viola, MBA, RHIA

Crystal Kallem (crystal.kallem@ahima.org) is director of practice leadership at AHIMA.

Article citation:
Kallem, Crystal. "Data Stewardship: Global Recommendations for Local Action" *Journal of AHIMA* 79, no.9 (September 2008): 58-59;63.