Health Data Access, Use, and Control

Save to myBoK

This practice brief has been retired. It is made available for historical purposes only.

Traditionally healthcare professionals have operated under the premise that patients own their medical and health information. When the information is recorded on paper or other hard media such as film or magnetic disk, that media is said to be the physical property of the healthcare entity that captured or recorded the information.

However, the nature of electronic health information-its ability to be transmitted, shared, and leveraged for a myriad of purposes-has resulted in new and greater uses of health data. A greater variety and number of organizations now hold healthcare data and employ it for uses other than direct patient care, the original purpose for which it was created. Even in the paper world, providers believe that they have the right to access and use the information for secondary uses if they own the physical media.

The increasing secondary use of health data raises the industry's clear need to define stakeholder rights and responsibilities. It also requires an increasing focus on the importance of data stewardship at the most local levels. Both are essential steps in creating consumer trust in the exchange of personal health information and in putting consumers at the center of decisions made about their information.

A Need to Redefine "Ownership"

Providers legitimately use health information for reimbursement, credentialing, legal defense, and quality management. Thus, patients have never had *exclusive* ownership of their health information, where ownership is defined as "the ability to exercise complete sovereignty over information-to disclose, sell, destroy, alter, or determine who shall have access to it at will."[1]

Many organizations that hold electronic health information contend that they have the right to access and use it for legitimate business purposes by virtue of the fact that they possess the information. Challenges arise, however, when accessing and using extremely personal health information conflicts with an organization's business purposes, many of which may never provide a direct or indirect benefit to the individual.

Because of these complexities, it is necessary to redefine the concept of "ownership" in terms of access, use, and control of health data by any entity that originates, creates, produces, or holds health information, whether that information is identifiable or not. "Who can do what to which data and under which circumstances" is really the central question that must be asked in determining the rights and responsibilities of each stakeholder.[2]

In addition to providers, health data are also captured and held by health plans, clearinghouses, payers, technology and service vendors, researchers, employers, financial service firms, and public health agencies. This diverse set of entities, along with the patient or individual, constitutes the body of stakeholders that must be concerned with health data access, use, and control.

In its report "Toward a National Framework for the Secondary Use of Health Data," the American Medical Informatics Association states that "the current lack of coherent policies and practices for the secondary use of health data presents a significant impediment to the goal of transforming the US health system." It also states that there is a growing need to "explicitly address questions concerning access and control of data throughout their life cycle" and "to develop appropriate policies for the secondary use of health data, recognizing that such policies are critical and complex."[3]

Delineating and understanding the rights and responsibilities of each stakeholder is the first step in developing policies and practices related to secondary uses of health information. These rights and responsibilities can then fill in the gaps between the individual's right to privacy and IT's capabilities and address such issues as personal control of health information; intellectual property rights when health information is involved; policies related to identity management; and societal requirements that

affect the individual's right of control, such as the need for public and population health data. These are just some examples of the very difficult issues that have come up in the transition to electronic health information.

Factors in the Secondary Use of Data

Currently, there is no universal authoritative source, law, or regulation that addresses and defines stakeholder rights and responsibilities. There is clearly a need to develop standards, policies, and practices to better define and reflect the rights and responsibilities of stakeholders. The development of these principles can be guided by several factors that have a bearing in determining what these rights and responsibilities should be with regard to secondary data access, use, and control.

Status as a Legal or Business Record

ISO defines business records as "information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business."[4] The International Council on Archives Committee on Electronic Records defines a record as "a specific piece of recorded information generated, collected or received in the initiation, conduct or completion of an activity and that comprises sufficient content, context and structure to provide proof or evidence of that activity."[5]

It is important to recognize that not all health data and information are necessarily a business or legal record. For example, an individual may choose to create and maintain a personal health record on his or her employer's Web site. This personal health record cannot be considered a business record of the employer even though it is maintained on the employer's Web site, because the information does not meet the ISO criteria of "created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business."

On the other hand, a report that contains aggregated or summarized data generated by the employer from personal health records of many employees may be considered a business record created by the employer. The level of the data-whether it is a discrete record or an aggregate of many discrete records-is a factor in determining who may access it and how it can be used.

Status as a legal or business record implies that a stakeholder has greater rights to access, use, and control the information than a situation in which the information cannot be considered a business record.

De-identification

Adequate de-identification can be difficult to achieve, and certain levels of de-identification can render data useless.[6] However, the extent to which the data are de-identified can determine which rights and responsibilities apply to information holders.

Full de-identification with no ability for re-identification allows the information to be accessed and used to a much larger extent because there is less need to control it to protect privacy. Information that has been de-identified with no capability to re-identify can be readily disclosed, sold, or published without risk of breaching personal right to privacy.

Contracts and Business Agreements

Contracts and business agreements that specify what information may be accessed and how it is to be used and protected also play a role in how each stakeholder manages health information and data in its possession. These contracts can take many forms, including patient or individual consents, data use agreements, business associate agreements, or nondisclosure clauses.

A special agreement related to data and information use is the so-called opt-in or opt-out agreement, where the patient or individual positively affirms or declines to let specific information be used for specific purposes.

State and Federal Laws and Regulations

Laws and regulations such as HIPAA, federal drug and alcohol abuse rules, and state laws and regulations related to mental health, HIV/AIDS, abuse or neglect, population health, and genetic nondiscrimination frequently address rights and responsibilities related to access, use, and control of health information.

However, such laws often do not apply to all stakeholders. They may be limited in scope or fail to address secondary uses of health information. The limited extent that these laws do address policies and practices for stakeholders handling health information can serve as a model for entities seeking guidance in the development of policies and practices.

Potential for Discriminatory Use

Secondary uses of health information to make employment, insurance, or financial decisions may carry the potential for discrimination against individuals.[7] The more downstream the use is from the original purpose for the information, the greater the potential.

Whether or not it is mandated by law, users of health information should obtain individual consent, limit access and use of the information to relevant purposes, and ensure that the information is not used unfairly or that it negatively affects the individual. Individuals will not participate in a system that they perceive to be unsafe or not in their best interest.

Individual Control

Although helpful, the preceding factors do not go far enough in addressing the gaps in identifying and understanding stakeholder rights and responsibilities. Control of personal health information must rest with the individual to whom information pertains and must be reflected or expressed in public policy and the organizational practices and processes of business and institutional stakeholders.

The National Committee on Vital and Health Statistics addressed the issue of controlling personal health information in a June 2006 report to the Health and Human Services secretary regarding privacy and confidentiality in the nationwide health information network (NHIN). The report noted:

> Deciding on the appropriate level of individual control over personal health information accessible via the NHIN involves balancing important interests, such as the desire of some individuals to be able to control their personal health information and the need to document accurately medical history and treatment; the desire for a system that is flexible and the need to avoid a system that is too complicated; the desire to increase individual choice, and the desire to reduce complexity and the costs imposed on providers, payers, and other stakeholders.[8]

Beyond the questions of how records are kept (paper versus electronic) and whether participation in the NHIN should be mandatory, this report questions the extent to which individuals should control their health information. Opponents of the individual's right to control personal health information offer several arguments: that such rights would jeopardize the integrity of health records because individuals could make substantive changes to the content; that it could result in poor care decisions due to incomplete or inaccessible information by healthcare providers; and that it could result in malpractice liability due to incomplete or inaccessible health information.

Individuals must have limited rights to control their personal health information. Examples of these limited rights include the right to request amendments or corrections (but not the right to alter or delete records) and the right to control disclosures and restrict access by third parties (but not when required by law such as for public health reasons or population health studies). Without such control, individuals will be reluctant to share health information with healthcare providers. This will result in compromised healthcare and an NHIN that is incomplete and inaccurate.

In the absence of universal regulations and policies, we must address the critical and ongoing role of stewardship in protecting patient privacy and placing patients at the center of decisions to use their health information.

Stewardship of Health Information

Stewardship is the process of managing what belongs to another. It requires professional diligence if consumer trust is to be built around data management in healthcare's developing electronic environment.

Even as industry standards emerge and are harmonized, adoption of practices fully respectful of the healthcare consumer and other stakeholders depends, at least in part, on altruistic decision making by originators and holders of data. Stewardship represents a *willingness* to do what is not explicitly required or readily obvious because it is the right, and in some cases, ethical

choice. Proper administration of data access, use, and control operations is synonymous with proper administration of privacy protections.

While the industry lacks uniform data access, use, and control requirements, the level of protection afforded an individual's data is significantly dependent on stewardship at the local level. Many questions remain unanswered about how to ensure consistent control wherever data exist, about the appropriate use of secondary data, and how to give the consumer a voice.

Over time-even after definitions and processes have been standardized-the greatest protections related to access, use, and control of protected health information will be based on administrative handling and responsible human intervention. Any assurances will be vested in organizational philosophy and due diligence manifesting in policies, procedures, practices, and consistent enforcement and follow-through.

Technology introduces new issues and complexities not present in the paper environment because information becomes more pervasive. Some protective practices can be implemented through technology safeguards or with technology assistance. Others can be encouraged with user-friendly technology features. Still more are only as effective as the due diligence and tolerance exercised by data originators and holders within healthcare organizations across the continuum.

Contractual obligations are usually legally testable. Laws and regulations, though legally testable, may lack compliance monitoring and enforcement. Where best practices offer the only guidance, the organization is in full control to create-or not create-what the individual and stakeholders have the right to expect.

When current ambiguity is replaced by an electronic environment of complete standards, heightened regulations, and consistent business practices, stewardship factors affecting data access, use, and control will remain critical. Regardless of the degree of formalized industry control, the need for ongoing respect of stewardship responsibilities will not diminish. Even holders of health information not bound by legal or regulatory compliance directives have an ethical obligation to protect patient health information as any formally bound entity.

Without it we will not establish the trust necessary to implement the electronic health record, health information exchange, and resulting improvements in quality of care, patient safety, homeland security, and administrative simplification. (See "Stewardship Guidelines for Stakeholders" [below] for 15 actions that lead to responsible handling of patient health information.)

Stewardship Guidelines for Stakeholders

- Honor the patient-centric direction of the national agenda; set up policies that keep the patient in control of his or her own data wherever possible.
- Initiate data creation, import, and flow processes respectful of the data quality attributes delineated in AHIMA's position statement "Quality Healthcare Data and Information." Ensure appropriate use of quality data by and for the individual, the organization, and the industry to improve quality of care, patient safety, and public health.
- Anticipate broader, external data sharing and health information exchange when establishing an organizational position with data access, use, and control.
- Create a top-down organizational culture that places sound data and information management principles (HIM and IT) at the foundation of your organization's stewardship philosophy. Set proactive approaches toward optimal protections, rather than leave individual victims and the legal system to find holes in your stewardship diligence.
- Adopt a philosophy of reward for staff diligence in protecting health information rather than fear when problems are identified.
- Create a system architecture that maximizes security safeguards and technology benefits that force, help to enforce, and encourage privacy protections and policies. Purchase only certified EHR products aligned with industry-recognized functionality and security criteria.
- Establish internal policies governing your stakeholder responsibilities for optimal data access, use, and control regardless of the absence of external mandates and requirements. Ensure inclusion of antidiscrimination policies.
- Aggressively employ accreditation standards and regulatory and legal requirements on the federal, state, and local levels. Use HIPAA and Joint Commission standards as baseline expectations regardless of their relevance to your organization.
- Take a noncompromising position toward optimal interpretation of nonspecific regulations and laws. Set up clear, enforceable policies and practices.
- Establish enforcement policies with consistent interpretation and application to staff and business associates in all roles and on all levels. Follow through on punitive steps for proven noncompliance. Make outcomes visible as appropriate and educational.
- Establish or expand the responsibilities of an ethics committee to manage and interpret issues requiring judgment calls and professional accountability and reporting.

- Extend privacy and security principles into all aspects of the data use, access, and control program adopted in the organization. Periodically review and update the program.
- Develop processes to challenge requests for health information that appear to seek more information than is necessary to serve the purpose of the request.
- Establish policies regarding retention and destruction of data when used or created for secondary use. When possible, ensure those policies are enforced after the original purpose is fulfilled and data are no longer needed.
- Educate consumers about their rights and responsibilities regarding the use of their personal health information, including the decisions that will help improve healthcare delivery at the point of care through the availability of information; how to become knowledgeable of and exercise their regulatory and legal rights; how to help keep their health information accurate; and tips on detecting fraud.

Conclusion

The gaps in the current national system of data access, use, and control contribute to the confusion of ownership issues in health information. The table "Stakeholders' Rights and Responsibilities of Protected Health Information" illustrates what policies have been established on a national level, where they are needed, and the necessary stewardship principles for each.

Evolving issues such as health record banking, implementation of health information exchanges, and the growing use of personal health records will change this landscape significantly in the near future. Issues related to data access, use, and control will require ongoing monitoring by stakeholders.

Overall, we should approach the application of stewardship by first recognizing that healthcare is becoming increasingly patient-centered, and we must put patients at the center of the decisions we make about their information. This focus requires organizational commitment to continuously review policies, procedures, and practices in order that they clearly reflect the organization's commitment. We must also reflect this philosophy in our consumer education, employee training, and policy and procedure enforcement.

Stakeholders' Rights and Responsibilities of Protected Health Information

Stakeholders		Access	Use	Control
Individual/Patient	**Rights**	To access protected health information (PHI) within 30 days.	With the right to access, the use is up to the patient.	Patient should understand all possible uses of data, including secondary use.
	Responsibilities			
Clinician	**Rights**	Appropriate members of work force have access to the information in order to carry out their duties.	To use or disclose for treatment, payment, or healthcare operations (unless authorization is specifically required). To disclose as required by law or for public health activities.	*No current national regulation policy exists. Apply stewardship principles to:* justify and explain treatment; identify legal record; identify designated record set.
	Responsibilities	Identify work force members who need access to PHI to carry out their duties. Identify the categories of	Make reasonable efforts to limit work force members' access to PHI needed to perform their duties.	Have policies and procedures in place to comply with the privacy and security rules.

		information they may access.	To use or disclose for treatment, payment, or healthcare operations. To disclose as required by law or for public health activities.	*No current national regulation policy exists. Apply stewardship principles to:* identify responsibilities of stakeholders upon sale or transfer of business.
Provider Organization	**Rights**	Appropriate members of work force have access to the information in order to carry out their duties.	To use or disclose for treatment, payment, or healthcare operations (unless authorization is specifically required). To disclose as required by law or for public health activities	*No current national regulation exists. Apply stewardship principles to:* justify and explain treatment; identify legal record; identify designated record set.
	Responsibilities	Identify work force members who need access to PHI to carry out their duties. Identify the categories of information they may access.	Make reasonable efforts to limit work force members' access to PHI needed to perform their duties. To use or disclose for treatment, payment, or healthcare operations. To disclose as required by law or for public health activities.	Have policies and procedures in place to comply with the privacy and security rules. *No current national regulation policy exists. Apply stewardship principles to:* identify responsibilities of stakeholders upon sale or transfer of business.
Referral clinician or provider	**Rights**	Appropriate members of work force have access to the information in order to carry out their duties.	To use or disclose for treatment, payment, or healthcare operations (unless authorization is specifically required). To disclose as required by law or for public health activities.	*No current national regulation policy exists. Apply stewardship principles to:* justify and explain treatment; identify legal record; identify designated record set.
	Responsibilities	Identify work force members who need access to PHI to carry out their duties. Identify the categories of information they may access.	Make reasonable efforts to limit work force members' access to PHI needed to perform their duties. To use or disclose for treatment, payment, or healthcare operations. To disclose as required by law or for public health activities.	Have policies and procedures in place to comply with the privacy and security rules. *No current national regulation policy exists. Apply stewardship principles to:* identify responsibilities of stakeholders upon sale or transfer of business

PHR Service Provider	**Rights**	*No current national regulation policy exists. Apply stewardship principles to:* outline policy that allows only appropriate members of work force to have access to PHI in order to carry out their duties.	*No current national regulation policy exists. Apply stewardship principles to:* limit use or disclosure for business operations (unless authorization is specifically required). Disclosure as required by law.	*No current national regulation policy exists. Apply stewardship principles to:* Outline policy that PHI should be under patient control.
	Responsibilities	*No current national regulation policy exists. Apply stewardship principles to:* identify work force members who need access to PHI to carry out their duties; identify the categories of information they may access.	*No current national regulation policy exists. Apply stewardship principles to:* make reasonable efforts to limit work force members' access to PHI needed to perform their duties; to use or disclose for business operations; to disclose as required by law.	*No current national regulation policy exists. Apply stewardship principles to:* outline policies and procedures to comply with the privacy and security rules. *No current national regulation policy exists. Apply stewardship principles to:* identify responsibilities of stakeholders upon sale or transfer of business
Insurance Company	**Rights**	Appropriate members of work force have access to the information in order to carry out their duties.	To use or disclose for treatment, payment, or healthcare operations (unless authorization is specifically required). To disclose as required by law.	*No current national regulation policy exists. Apply stewardship principles to:* justify and explain treatment; identify legal record; identify designated record set.
	Responsibilities	Identify work force members who need access to PHI to carry out their duties. Identify the categories of information they may access.	Make reasonable efforts to limit work force members' access to PHI needed to perform their duties. To use or disclose for treatment, payment, or healthcare operations. To disclose as required by law.	Have policies and procedures in place to comply with the privacy and security rules. *No current national regulation policy exists. Apply stewardship principles to:* identify responsibilities of stakeholders upon sale or transfer of business

Health Data Exchange	**Rights**	*No current national regulation policy exits. Apply stewardship principles to:* outline a policy that allows only appropriate members of work force have access to the information in order to carry out their duties.	*No current national regulation policy exists. Apply stewardship principles to:* limit use or disclosure for business operations (unless authorization is specifically required); disclose PHI as required by law.	*No current national regulation policy exists. Apply stewardship principles to:* justify and explain business/coverage decisions.
	Responsibilities	*No current national regulation policy exists. Apply stewardship principles to:* identify work force members who need access to PHI to carry out their duties; identify the categories of information they may access.	*No current national regulation policy exists. Apply stewardship principles to:* make reasonable efforts to limit the access of work force member to PHI needed to perform their duties; use or disclosure for business operations; disclose as required by law.	*No current national regulation policy exists. Apply stewardship principles to:* outline policies and procedures in place to comply with the privacy and security rules. *No current national regulation policy exists. Apply stewardship principles to:* identify responsibilities of stakeholders upon sale or transfer of business.
Health Data Bank	**Rights**	*No current national regulation policy exists. Apply stewardship principles to:* outline a policy that allows only appropriate members of work force have access to the information in order to carry out their duties.	*No current national regulation policy exists. Apply stewardship principles to:* limit use or disclosure for business operations (unless authorization is specifically required); disclose PHI as required by law.	*No current national regulation policy exists. Apply stewardship principles to:* justify and explain business/coverage decisions.
	Responsibilities	*No current national regulation policy exists. Apply stewardship principles to:* identify work force members who need access to PHI to carry out their duties; identify the categories of information they may access.	*No current national regulation policy exists. Apply stewardship principles to:* make reasonable efforts to limit the access of work force to PHI needed to perform their duties. Use or disclosure for business operations; disclose PHI as required by law	*No current national regulation policy exists. Apply stewardship principles to:* have policies and procedures in place to comply with the privacy and security rules. *No current national regulation policy exists. Apply stewardship principles to:* identify responsibilities of

				stakeholders upon sale or transfer of business
Business Associates of Covered Entitites	**Rights**	Appropriate members of work force have access to the information in order to carry out their duties.	To use or disclose for treatment, payment, or healthcare operations (unless authorization is specifically required). To disclose as required by law.	*No current national regulation policy exists. Apply stewardship principles to:* justify and explain business/coverage decisions.
	Responsibilities	Identify work force members who need access to PHI to carry out their duties. Identify the categories of information they may access.	Make reasonable efforts to limit the access of work force to PHI they need to perform their duties. Use or disclosure for business operations. To disclose as required by law	*No current national regulation policy exists. Apply stewardship principles to:* have policies and procedures in place to comply with the privacy and security rules. Return or destroy all PHI at the termination of the contract. *No current national regulation policy exists. Apply stewardship principles to:* identify responsibilities of stakeholders upon sale or transfer of business.

Reference

Health Insurance Portability and Accountability Act of 1996. Public Law 104-191. August 21, 1996.

Notes

1. Waller, Adele A., and Oscar L. Alcantara. “Ownership of Health Information in the Information Age.” *Journal of AHIMA* 69, no. 3 (March 1998): 28–38.
2. Ibid.
3. American Medical Informatics Association. “Toward a National Framework for the Secondary Use of Health Data.” September 2006. Available online at www.amia.org/inside/initiatives/healthdata.asp.
4. Quoted in Wikipedia. “Business Records.” Available online at http://en.wikipedia.org/wiki/Records_management. [see also: International Standards Office. "Terms and Definitions", *Information and Documentation - Records Management Part 1: General (ISO 15489-1)*, Geneva: ISO, 2001].
5. Quoted in Wikipedia. “Records Management.” Available online at http://en.wikipedia.org/wiki/Records_management. [see also: International Council on Archives, Committee on Electronic Records. *ICA Guide on Electronic Records*, Paris, 1997.]
6. Health Insurance Portability and Accountability Act of 1996. Public Law 104-191. 45 CFR § 164.514 (a).
7. National Committee on Vital and Health Statistics. “Privacy and Confidentiality in the Nationwide Health Information Network.” June 22, 2006. Available online at http://www.ncvhs.hhs.gov/060622lt.htm.
8. Ibid.

Prepared by

Jill Burrington-Brown, MS, RHIA, FAHIMA
Beth Hjort, RHIA, CHPS
Lydia Washington, MS, RHIA, CPHIMS

Acknowledgments

Jill Callahan Dennis, JD, RHIA
Donald T. Mon, PhD, FHIMSS
Dan Rode, MBA, FHFMA

Article citation:
Burrington-Brown, Jill; Hjort, Beth M.; Washington, Lydia. "Health Data Access, Use, and Control" *Journal of AHIMA* 78, no.5 (May 2007): 63-66.