Data Ownership Evolves with Technology

Save to myBoK

By Barbara Demster, MS, RHIA

Technology has transformed the world of health information management (HIM), bringing about change for many of the field's longstanding professional concepts and work methods. The classic rule of ownership in the words-on-paper era of health records was that "the paper (physical medium) belongs to the provider and the words (data/information) belong to the patient." Such a mantra is no longer feasible in the new electronic environment. Though words on paper are easier to control, physical records are also more difficult to share and manipulate. Electronic data, however, can easily be shared, manipulated, and proliferated. As a result of today's electronic health information environment, data ownership defined as sovereign control simply does not exist.

The value and benefits of patient data extends beyond the immediate bounds of patient care. Data can also be generated by a myriad of commercial products and services (i.e., applying technology in managing chronic disease). Ownership rights and, more importantly, access to the data can deliver cash to the bottom line.

Numerous federal and state laws provide rights of access under certain conditions for patients, families, government agencies, law enforcement officials, public health officials, and oversight entities, among others. Many of these same laws impose obligations on entities that have been traditionally considered owners along with business associates who use their patient data, such as health information exchanges (HIEs).

Technology Enhances Data

Technological advances like the Internet and mobile devices have enabled a new level of ease for data creation, proliferation, and access. The industry focus on standards development and interoperability-buttressed by regulatory mandates for electronic health records-has created an environment that facilitates rapid data growth, dissemination, and exchange. Information exchanges occur within, between, and among systems, regional health organizations, and the nationwide health information network. The implications for data ownership in this new environment are immense. Electronic data become redundant when they are passed and shared between providers and their systems. Data are mined and manipulated, which can impact data integrity. Data can also be hard to locate, preventing amendment, update, and correction opportunities.

Owning Modern Health Data

In order to understand data ownership, it is necessary to understand the nature of the data itself-the information life cycle and the workflow that carries data all the way from inception to the final stages of destruction. Questions to ask include:

- How is data created?
- How is the data modified or amended?
- How is it maintained physically and technically?
- How is it secured?
- What access controls are used-both administrative and technical?
- What are the practices for timeliness, exchange, matching/linking, use and reuse, disclosure and re-disclosure, privacy protections, update, correction, amendment, quality control, integrity, retention, and destruction?

The list goes on. Gaining control over data in the world of technology requires a massive effort focused on strong strategies of governance and stewardship.

"Data governance" and "data stewardship" are terms frequently used in conjunction with data ownership. They are closely related concepts that have expanded in usage and concept in the digital age in an effort to gain control over data infrastructure and maintenance. Data ownership, governance, and stewardship are closely intertwined and sometimes used interchangeably.

Data management authors Berson and Dubov define data governance as "a process focused on managing the quality, consistency, usability, security, and availability of information."[1] They also differentiate data stewards from data owners, writing, "Data stewards do not own the data and do not have complete control over its use. Their role is to ensure that adequate, agreed-upon quality metrics are maintained on a continuous basis." For some, data ownership is a subset of data governance.

Data Owners Must Act Responsibly

The Office for Civil Rights (OCR)-the enforcement agency for HIPAA privacy and security regulations-has found that mishandled data typically plays a part in their investigations. OCR reports that since HIPAA was implemented in 2003, the top three investigation types that lead to corrective action are:

1. Impermissible uses and disclosures
2. Safeguards
3. Access

Data owners are clearly leaving themselves at risk, exposing themselves to legal violations and subsequent enforcement penalties.

Healthcare attorney Adele Waller writes "…what is often the real question being asked when the question, 'Who owns health information?' arises (is) 'Who can do what to which data under what circumstances?'"[2]

The responsibility to control access to data and its use is considered a major function of a data owner. Data owners have the authority to authorize or deny access to data or its subparts. These decisions may be based on legal requirements (i.e., HIPAA, HITECH, GINA, state, and other federal laws), business policies and processes, patient authorization, or other factors.

The responsibility of a data owner is to think through the business processes of the data and address all business requirements. Prior to granting access, data owners must anticipate uses and disclosures of data to mitigate unforeseen manipulation or misuse.

Data owners are obliged to observe the various privacy rights afforded patients in state and federal law. As patient data pass from organization to organization through HIEs, they move farther away from the data creator and on to new owners who are also obliged by law to observe the patient's privacy rights.

The concept of "original" versus "copy" in the digital world is a challenge. New technology allows information to be tagged with the patient's privacy preferences in order to pass along the patient's wishes. As these data move across state lines or jurisdictions, new owners may be subject to different or conflicting privacy laws and consent requirements. In other words, the rules change even though the patient data have not.

Responsibilities of data ownership include the assurance of data confidentiality, integrity, and availability. These depend heavily on the data governance processes defined by the organization, as well as the data stewards who maintain these processes.

Data Management Questions Change

HIE raises a host of new questions when it comes to data ownership. The question "Who has the original?" has changed to:

1. "What is an original?"
2. "Does it matter?"
3. "Who owns or controls the patient record consolidated from multiple stakeholders?"
4. "What about data privacy, access control, accuracy, and integrity?"
5. "How do data owners relate to their data sharing partners and business associates for updating and notification of updates?"
6. "How is a data correction initiated or received in all of the new proliferated forms and locations?"

Effective data management begins with a comprehensive understanding of the challenges and requirements necessary for a solid data governance model supported by strong policies and procedures.

Data Ownership Definition Evolving

The definition of data ownership currently remains unclear. However, the need for data ownership is continuously in demand. Owners must assess their ownership responsibilities in relation to the data they create, collect, mine, store, and distribute. They should develop a strong data governance strategy that includes policies, processes, accountabilities, enforcement, and sanctions.

Collaboration with data stewards to define information requirements is also necessary. Data owners must take steps to develop and enforce policies for access, use, and disclosure, and work to ensure information quality, integrity, and availability needs are met.

Data must be considered a corporate asset. The C-suite must address their responsibilities with strong and informed support, funding adequate budgets to hire qualified staff and to purchase thoroughly vetted information systems to ensure the achievement of current and future ownership needs.

Notes

1. Berson, Alex, and Larry Dubov. *Master Data Management and Customer Data Integration for the Global Enterprise*. McGraw-Hill, 2007.
2. Waller, Adele A. and Oscar L. Alcantara. "Bridging the Gaps: An Assessment of Culture in an Integrated System." *Journal of AHIMA* 69, no. 2 (1998): 28-38.

References

Fernandes, Lorraine; O'Connor, Michele. "Data Governance and Data Stewardship: Critical Issues in the Move toward EHRs and HIE." *Journal of AHIMA* 80, no.5 (May 2009): 36-39.

Barbara Demster (bdemster51@gmail.com) is chief compliance officer at Benchmark Consulting.

Article citation:
Demster, Barbara. "Data Ownership Evolves with Technology" *Journal of AHIMA* 83, no.9 (September 2012): 52-53.