Evaluating the Information Governance Principles for Healthcare: Integrity and Protection

By Galina Datskovsky, PhD; Ron Hedges, JD; Sofia Empel, PhD; and Lydia Washington, MS, RHIA

Editor's note: This is the second in a series of four articles that discuss the eight Information Governance Principles for Healthcare.

AHIMA's new Information Governance Principles for Healthcare (IGPHC) provides a framework for healthcare organizations to enhance their ability to leverage information in order to achieve the organization's goals, and conduct their operations effectively while ensuring compliance with legal requirements and other duties and responsibilities.

IGPHC is a set of eight principles that, when considered in whole or in part, are intended to inform an organization's information governance strategy. This article is the second of four that explores the meaning and intent of the principles, two at a time.

Integrity Principle

The principle of integrity states that an information governance (IG) program should be constructed and managed such that "the organization has a reasonable and suitable guarantee of authenticity and reliability." In healthcare, integrity of information means that an organization has the ability to prove that information is authentic, timely, accurate, and complete. This is a fundamental expectation from patients, providers, and other stakeholders such as regulatory agencies.

This principle recognizes that an information governance program should include:

- Adherence to the organization's policies and procedures
- Appropriate workforce training on information management and governance
- Reliability of information
- Admissibility of records for litigation purposes
- Acceptable audit trails
- Reliability of systems that control information

Why are these elements important for good information governance? Consistent practices that assure the quality of information must be integrated into every step in the information lifecycle. For example, it is critical that organizations determine their responsibilities and processes for both internally created information as well as that which is received from external sources. The latter, however, might include taking additional steps that are necessary to identify and classify the information before adding it to a patient's health record.

Adherence to IG policies and procedures helps an organization not only comply with regulatory and legal requirements, but more importantly, assure patient safety and care quality. In addition, workforce training empowers individuals to comply with those policies and emphasizes their importance.

Audit trails document activities related to information, and therefore reinforce the reliability and integrity of that information. Likewise, information cannot be reliable unless the technology infrastructure on which it is created, used, maintained, and stored is reliable. Therefore, an organization should monitor its infrastructure for deficiencies, and when necessary take appropriate action to correct problems and mitigate risks.

Integrity provides trust that the information is authentic. An authentic record is one that is proven to:

- Be what it purports to be
- Has been sent, received, or created by the person or system purported to have done so
- Has been sent, received, or created at the time purported

The principle of integrity seeks to assure the trustworthiness of information through the development and implementation of information governance processes and procedures by which information is generated, used, and maintained throughout its lifecycle.

Protection Principle

The principle of protection states that an IG program must provide "the appropriate levels of protection from breach, corruption, and loss… for information that is private, confidential, secret, classified, essential to business continuity, or otherwise requires protection." Given the intensely personal, sensitive, and life sustaining nature of health information, the principle of Protection has a special emphasis in healthcare.

Many healthcare organizations have established privacy and information security programs, and these should be integrated into the overall information governance program.

Protection takes various forms and may include:

- Active management of, and restriction of access to, information according to context
- Prevention of unauthorized information disclosure by clearly defining policies, creating safeguards, and then monitoring them to prevent leakage
- Securing final disposition of information, regardless of source or media
- Audit programs to validate whether sensitive information is handled in accordance with organizational policies and procedures and in compliance with applicable laws and practices

As part of their operations healthcare organizations must manage sensitive patient information in addition to administrative data. The principle of protection recognizes that information has varying degrees of sensitivity that must be categorized accordingly, and then must be safeguarded throughout its life span. In healthcare, information must be protected throughout the ecosystem, at the source and by all stakeholders.

Integrity and Protection Improve Trustworthiness

Trust is central to the integrity and protection of healthcare information. Users must be confident that the information on which decisions are based is what it purports to be, just as business people, regulators, and juries should have similar confidence. That confidence requires the information have integrity. Integrity itself requires that information be protected from, among other things, loss, theft, unauthorized access, or unauthorized change. The principles of integrity and protection operate together to create and maintain information that stakeholders, including patients, can have confidence in.

Integrity and Protection Improve IG

In the first installment of this series, the authors noted that "at its basic level, governance requires trust in decision makers and the decisions they make." The article then discussed the synergistic relationship between the principles of accountability and transparency in creating and maintaining that trust.

Similarly, governance requires trust in the information that a healthcare organization uses for business reasons, whether those reasons relate to patient care and treatment, patient or insurer billing, or, for that matter, the construction and maintenance of physical plants.

Information must have integrity to be useful and to be depended on for decision-making. That information must be protected to maintain integrity. Together, these principles enable information to be relied on. This synergy increases not only in the information, but also in the overall information governance program.

Link
Read the Full IGPHC Principles
www.ahima.org/topics/infogovernance

For a detailed look at all eight Information Governance Principles for Healthcare, as well as other information governance resources, visit www.ahima.org/topics/infogovernance.

Galina Datskovsky (gdatskovsky@gmail.com) is CEO, North America, at Covertix. Ron Hedges (r_hedges@live.com) is a former US Magistrate Judge in the District of New Jersey and is currently a writer, lecturer, and consultant on topics related to electronic information. Sofia Empel (sofia.empel@connolly.com) is director, information governance, at Connolly iHealth. Lydia Washington (lydia.washington@ahima.org) is senior director of HIM practice excellence at AHIMA.

Article citation:
Datskovsky, Galina; Hedges, Ron; Empel, Sofia; Washington, Lydia. "Evaluating the Information Governance Principles for Healthcare: Integrity and Protection" *Journal of AHIMA* 86, no.4 (April 2015): 48-49.