Managing the Security of Information (Resolution)

Save to myBoK

Resolution from the 1997 House of Delegates

Background Information

Changes in the healthcare delivery system and advances in technology are having a profound impact on HIM. More data than ever are collected, stored, and displayed in electronic form. Until very recently, laboratory data were the only types of information available online. Today in some facilities, entire medical record systems are computerized. Technology development has brought us faster computer chips, less expensive hardware, laptop computers, palmtops, and now intranets and the Internet. All this technology is being applied in healthcare.

Not only is technology transforming information management, but the demand for information has never been greater. Mergers, acquisitions, managed care contracts, and fee-for-service agreements send administrators clamoring for data. Best practices, clinical pathways, outcomes measurement, and health status monitoring place demands on clinical data that are almost impossible to meet in a paper environment. Additionally, the needs of a truly integrated delivery system, in which patient information is available at any site at any time of the day or night, create an expectation of information that even most existing computer networks are not designed to meet.

This weighty demand to find a computerized patient record solution has surpassed the industry's ability to keep information secure and assuring the personal privacy on which healthcare is based. The industry must assume leadership in addressing these issues or prepare for strict regulation, lawsuits, and consumer dissatisfaction.

Resolution

Topic:	Managing the Security of Health Information
Intent:	Improve the security of health information by preparing AHIMA members to take leadership roles
Addressed to:	All HIM professionals and AHIMA's strategic partners
Originator:	AHIMA Information Security Task Force
Approved by:	1997 House of Delegates
Date:	October 19, 1997

Whereas, patients have a fundamental right to health information security;

Whereas, access to health information is necessary to provide care, improve outcomes, manage reimbursement, improve healthcare delivery, conduct research, and plan at all levels of healthcare delivery;

Whereas, health information must be kept in a secure and reliable manner that ensures its accuracy and integrity;

Whereas, HIM professionals have unique education and training in the principles of confidentiality and release of information;

Whereas, health information management professionals are required by AHIMA's Code of Ethics to protect the confidentiality of health information;

Whereas, AHIMA has a long tradition of advocacy and actively participates in the development of legislation and regulation that addresses information security and confidentiality;

Whereas, Vision 2006 calls for development of new roles for HIM professionals; and

Whereas, the current state of information security in healthcare does not assure a reasonable level of privacy for patients; therefore, be it

Resolved, That AHIMA and its component groups educate members and students to increase their understanding of information security principles and technologies and update members on the most current regulations, standards, and methodologies for securing health information; and

Resolved, That AHIMA members advocate patient privacy as an organizational priority and educate users of health information about the need for improved information security and the role HIM professionals have in securing information.

Source:
"Managing the Security of Information (Resolution from the 1997 House of Delegates)." *Journal of AHIMA* 69, no.1 (1998): insert before p.49.

Driving the Power of Knowledge