



Health Information Management Professionals Are Uniquely Qualified as Privacy and Security Officials

Approved – December 2007

The AHIMA Position

Since its formation in 1928, the American Health Information Management Association (AHIMA) has provided its members with education and training to help them protect patient privacy and the security of protected health information (PHI). AHIMA recognizes the public's right to accurate and confidential PHI and the need for advanced practices, processes, and standards that safeguard the confidentiality, privacy, and security of PHI. Credentialed health information management (HIM) professionals—with their academic preparation, work experience, commitment to patient advocacy, and professional code of ethics—are uniquely qualified to assume designated privacy and security official positions as required by the Health Insurance Portability and Accountability Act (HIPAA) privacy rule.

Facts That Support the AHIMA Position

With the advent of electronic health records, it is critical to ensure the confidence of healthcare consumers. HIM professionals have been long recognized as key resources for managing health information and providing direction for appropriate use and disclosure of protected health information (PHI).

HIM professionals establish and maintain organizational privacy policies and procedures, develop processes for appropriate access to PHI, author and present confidentiality education and training programs, and develop compliant authorization processes and practices that respond to individual privacy and security concerns.

This unique positioning enables HIM professionals to take on leadership roles in complying with state and federal privacy and health information laws as well as accreditation and research standards. They are also equipped to develop appropriate organizational initiatives and make ethical decisions regarding the confidentiality, integrity, and availability of PHI.

HIM professionals understand that keeping patient health information secure requires a strong understanding of the privacy policy and information management principles necessary to design appropriate security strategies.

HIPAA privacy and security rules mandate that covered entities (healthcare providers, health plans, and healthcare clearinghouses) designate a privacy official *and* a security official to address organizational privacy and security issues. HIM professionals have the specialized skills that uniquely qualify them to assume the role both of privacy official and/or security official and:

- Understand the decision-making processes throughout healthcare that rely on health information for treatment, payment, and healthcare operations, as well as public health and research
- Map and direct the flow of health information within healthcare organizations and throughout the healthcare delivery system
- Apply HIM principles to health and business record management in all its forms
- Understand the content of health information in its clinical, research, and business contexts
- Apply advancing technologies used to collect, access, store, protect, and transmit information in all media and formats
- Establish and recognize best practices in the management of privacy and security of PHI
- Manage healthcare organizations' disclosure or release of information processes
- Advocate for the individual relative to the privacy and security of paper or electronic PHI
- Live by a Professional Code of Ethics

Coursework that prepares HIM professionals to become certified in healthcare privacy and security is part of the curriculum of all accredited academic programs for health information administrators and health information technicians.

Background

Quality healthcare relies on complete, accurate health information, at every stage of its delivery, whether on paper or in an electronic format. Health information has value to the patient it describes, the provider it informs, the organizations it connects, and the population health system it supports throughout American society.

In addition to safeguarding confidentiality and security, patient health information must be protected as a valuable organizational asset vital to healthcare delivery, payment, and operational functions, as well as research and, most important, population health.

HIM is a complex task, with confidentiality, privacy, and security concerns changing in size and shape as technology increases the availability of, and access to, patient health information.

Issues related to the use and disclosure of information are complicated by conflicting federal and state regulations, lack of consistency in state regulations, and variations in organizational interpretations and practices. Even more complicated are issues related to research and the need to access PHI without patient authorization under difficult but appropriate circumstances.

Documented cases of the use of health information to make decisions about hiring, termination, and loan approval and to develop consumer marketing have sensitized the public to the risks of sharing information with healthcare providers and health plans. Increasingly reported incidents of identity theft, misuse of data, and loss of patient information in the healthcare industry have reinforced public awareness of the vulnerability of personal information as collected.

AHIMA is the premier association of health information management (HIM) professionals. AHIMA's 51,000 members are dedicated to the effective management of personal health information needed to deliver quality healthcare to the public. Founded in 1928 to improve the quality of medical records, AHIMA is committed to advancing the HIM profession in an increasingly electronic and global environment through leadership in advocacy, education, certification, and lifelong learning.

www.ahima.org