



Statement on the Confidentiality, Privacy, and Security of Health Records

Approved—December 2007

The AHIMA Position

The health information management (HIM) profession and the American Health Information Management Association (AHIMA) believe confidentiality, privacy, and security are essential components of a viable health record, reliable health information exchange, and the fostering of trust between healthcare consumers and healthcare providers. For over 80 years, HIM professionals have set the standard for protecting patients' right to confidential health information while promoting the integrity of information practices.

AHIMA calls upon the healthcare and information technology industries, relevant government agencies, federal legislators, employers, and consumers, to ensure that uniform and consistent confidentiality, privacy, and security protections are established and that technology is adequately used to appropriately protect personal health information in every format. Such protections must allow for the safe and appropriate creation, storage, and transfer of private health information so that the integrity of the data itself is protected and used only for its intended purposes.

AHIMA, furthermore, calls for the establishment of uniform privacy legislation that ensures that all individuals are secure from inappropriate discrimination on the basis of their health information and secure from the intentional misuse of their personal health information in whatever form it resides or wherever it is collected, utilized, transferred, or rests. Discrimination on the basis of health information or the intentional misuse of personal health information should not be tolerated and must be aggressively prosecuted and punished.

Healthcare needs and healthcare services should not be constrained by political boundaries. Uniform and consistent laws and regulations designed to protect the confidentiality, privacy, and security of health information are necessary to allow for healthcare services to be freely offered, conducted, received, and reimbursed nationwide. These laws and regulations must be readily understood, easily administered, and consistently applied in order to protect confidentiality and security of health information without becoming a barrier to healthcare delivery or the appropriate use of healthcare secondary data. Laws and regulations providing protection for personal health information must apply wherever such information is collected, stored, utilized or transferred, whether or not the organization is covered by the Health Insurance Portability and Accountability Act (HIPAA).

Facts That Support the AHIMA Position

A patient's health information can exist in various identifiable formats: paper, film, electronic, or a hybrid of two or more formats. This health information may be maintained by healthcare providers, healthcare plans, or health insurance payers as well as employers, government agencies, or any of a number of other public or private entities, or in personal health records maintained by individual patients. Many of these

entities are covered by inadequate healthcare confidentiality and privacy laws or regulations or are not covered at all.

However, there are circumstances when a legitimate public need to share health information arises, even times when information that can identify a specific individual needs to be shared: to protect public health, improve quality, monitor bioterrorism, or prevent medical fraud. An individual's right to privacy must be balanced against the public's right to be safe and the need for nationwide health information exchange capability. Yet privacy can never be sacrificed for expediency.

There are many—some argue too many—state and federal laws that cover health information confidentiality, privacy, and security, including HIPAA. The Health Information Security and Privacy Collaboration project identified instances where numerous and sometimes conflicting laws existed within a single state. It is not unusual for healthcare entities and individuals seeking healthcare services to find themselves covered by myriad overlapping—and sometimes conflicting—laws and regulations, only to have matters further complicated by overlapping jurisdictions. This type of legal and regulatory labyrinth makes it just as difficult for healthcare organizations to comply with laws and regulations as it is for government agencies to monitor their compliance. The result is an atmosphere of fear and caution that can, in some cases, jeopardize the provision of essential healthcare services.

These same conflicting laws, regulations, and practices have also created barriers to the adoption of a standard electronic health record (EHR) and health information exchange (HIE). While federal and state governments, accrediting organizations, and others are addressing the many policy and technology combinations for confidentiality and security needs, it is important to find solutions that do not create further barriers to the adoption of standard EHRs and HIE and that provide the level of health information, confidentiality, and trust demanded by the vast majority of America's healthcare consumers.

Trust is essential for the health information collected in a health record to serve as a complete and accurate foundation not only for clinical care but as the basis for research, public health, quality measurement, reimbursement, and policy making—all components of population health. In any medical setting, healthcare consumers need to be confident that their personal health information is protected and that identifiable information will be used only for purposes authorized or otherwise required by law. Unfortunately, patient surveys and other reports indicate their fear that they may be harmed or discriminated against through the intentional misuse of their personal health information. As a result, patient confidence is under fire almost daily, despite significant steps taken to protect their data.

There are no infallible means to ensure absolute respect and protection for the confidentiality and integrity of a patient's personal health information. But healthcare consumer trust can only be achieved and maintained if uniform laws and regulations are in place and violators are aggressively prosecuted.

AHIMA Recommendations

AHIMA believes that privacy, confidentiality, and security of health information will be achieved when:

- Patients and healthcare professionals trust and are confident that the collection and use of health information will only be used legitimately, be uniform everywhere and every time for everyone, apply everywhere personal health information resides, and protect individuals against inappropriate discrimination or harm from intentional misuse.

- Confidentiality and security protections are uniform and set a high standard throughout the country for fair, reasonable, and uniform health information practices that respect the rights of the individual and the public and apply to the medium in which such information is stored, transferred, or accessed.
- Confidentiality, privacy, and security laws and regulations are conscientiously enforced, and those who break these laws or ignore these regulations face vigorous prosecution and serious penalties for their offenses.
- Individuals will have the right to access their health information in any setting and with minimal limits; have an understanding of their privacy rights and options for that setting; be notified about all information practices concerning their information, and have the right to appropriately challenge the accuracy of their health information.
- Individuals, professionals and private entities, have a clear and understandable perspective on uniform law, regulations, and protections so that problems related to “overlaps,” “gaps,” and jurisdictional coverage will be eliminated, protection maximized, and trust built into the interaction.
- Individuals and clinicians contribute to the data contained in the record to make decisions based on sound clinical evidence, as well as the most current personalized medicine and genetics information. The information is only available to those caring for the patient, and on a limited basis, to others as appropriate for payment, operations, and research purposes.
- When security breaches occur, individuals receive timely notification in order to protect the confidentiality of their personal health information from being compromised.
- Credentialed HIM professionals, given their training and education in privacy and information release and HIM, are considered the primary custodians of health information and principal experts in maintaining the privacy, confidentiality, and security of information in the healthcare industry.

The American Health Information Management Association (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 health care 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