Testimony of the California Health Information Association

to the
Joint Hearing of the Select Committee on International Trade Policy and State Legislation
and the
Senate Business and Professions Committee
March 9, 2004

OPENING COMMENTS:

Chairman Figueroa, members of the Joint Committees, ladies and gentlemen, good morning. I am LaVonne LaMoureaux, Executive Director of the California Health Information Association (CHIA). On behalf of the Association, thank you for allowing us this opportunity to provide input on the privacy implications when health information is outsourced to other countries for transcription or other data processing activities.

CHIA is a non-profit association of over 3,000 of California’s credentialed health information management professionals. CHIA is a component state association of the American Health Information Management Association (AHIMA). Our members manage patient information in healthcare provider, health plan, government, and private organizations. Health information management professionals, relevant to our comments today, are actively involved in the development, implementation and management of electronic health record (EHR) systems and database systems; they are often those who manage the medical transcription services for healthcare organizations, and are often designated as the Privacy Officer in their healthcare organization. Health information management professionals strive to promote and protect the confidentiality and security of health records and health information.

As health information management professionals, we share your concern with the potential risks to patient privacy that may occur when protected health information is sent offshore for transcription or other data processing activities. The incident that occurred last October when a foreign-based transcriptionist employed by an outsourcing firm threatened to expose identifiable patient information on the Internet should not have happened. Technology and business practices available today could have prevented the transcriptionist from knowing the identity of the individuals whose information she was processing, could have prevented her from being able to hold the information on her own computer’s hard drive, and could have prevented her from being able to carry through with a threat to post transcribed reports onto the Internet.

WHY USE OFFSHORE TRANSCRIPTIONISTS?

Why would a healthcare provider, or contract vendor, use offshore transcriptionists? The main reason is that the demand for qualified medical transcriptionists in the U.S. has increased dramatically in recent years and there just are not enough qualified workers in the U.S. to do this important job.

The main driving force behind the increasing demand for transcriptionists is the rise of the electronic health record (EHR). These systems are populated with digitized medical record reports that are first dictated then transcribed. As the number of EHR systems increases, the volume of transcribed medical reports needed to support these systems grows proportionally.

Secondly, the expectations of healthcare providers for quicker turnaround times and legible documentation have increased significantly in recent years. Only a few years ago it was acceptable for some reports to be transcribed and returned to the provider in 48 hours or even longer. This time frame has shortened to where now an acceptable turnaround time for even the more “routine” medical reports is 4 to 6 hours (even shorter in some cases). This trend is a result of several factors: the healthcare providers’ efforts to improve patient care, the tightening up of standards by accrediting and regulating groups, and healthcare providers’ desire to deter
costly malpractice litigation. Quick turnaround time for transcribed reports means, for example, that an Emergency Department report dictated at 2 a.m. in the U.S. can be transcribed by an offshore transcriptionist within a 4-hour time requirement and be available to the patient’s private physician for early morning rounds or for follow-up care in his/her office. Having the reports available greatly improves communication between providers and results in improved patient care.

Additionally, there are increased pressures from payers for more detailed documentation to support charges for services. This means that many types of medical reports, such as emergency room reports, clinic notes, daily progress notes, physician’s office records, and others are now being dictated that previously were handwritten.

There has long been a shortage of qualified transcriptionists in the U.S., but the shortage has been greatly exacerbated by this increasing volume of dictation and by the demands for shorter turnaround times.

OTHER HEALTH INFORMATION FUNCTIONS THAT CAN BE OUTSOURCED

Transcription is not the only task that healthcare and related organizations can outsource. With the increasing development and use of electronic health records, emerging technologies and Internet communications, it is now possible to outsource other tasks that require access to the medical record information. These include coding of medical records, medical record abstracting for data reporting and research, claims management and other specialized functions. These functions are performed by medical record technicians. The US Department of Labor estimates that 97,000 new health information technicians will be needed by the end of this decade to meet the need. There are not enough skilled medical record technicians to meet forecasted demands nor are there adequate measures in place to remedy the shortage. In California, we have only eight accredited programs that teach health information technology. The one school that has a distance learning program via the Internet has a long waiting list. While CHIA and AHIMA have worked to encourage accredited programs, the community colleges in California strapped financially and so new programs have not been forthcoming.

INFORMATION TECHNOLOGY AND SECURITY FOR OUTSOURCING

Before protected health information is permitted to be sent offshore, technology systems and procedures should first be place that can adequately safeguard the privacy of text, voice and image files from unauthorized access, alteration, use or disclosure. Information and communication technology (ICT) now make it possible to outsource information with greater security than ever before and can prevent the type of incident that occurred last October in the UCSF case.

Not only is the industry outsourcing information processing to address workforce shortages, it also is using outsourcing as a cost control strategy enabling health care organizations to redirect scarce staff resources. It is estimated that 10% of medical transcription is currently being done outside the U.S. Rather than prohibit U.S. healthcare providers, payers or outsourcing companies from sending information overseas regardless of what measures are in place to ensure the privacy and security of the process, we urge enforcement of the privacy and security regulations.

It would be counterproductive to health care organizations if new state laws are established that make it impractical for national outsourcing companies to do business within a particular state. Further, many healthcare systems operate in a number of states. We urge our legislators to think about national and global business structures when addressing issues relating to health information as it is no longer a local issue.

Legislation that would call for institutions to first explain the potential for outsourcing to the patient and allow them to opt-out would be extraordinarily difficult to administer, would increase administrative costs, and would essentially require entities to “turn off” automated dictation-to-transcription systems. Such a requirement would affect the timely delivery of patient care services and have enormous cost consequences.
It is important for legislators to make policy decisions that promote the use of information and communications technology. Bringing healthcare further into the information age will have significant long-term benefits for the quality, safety and cost effectiveness of care by enabling important advances in information security that are currently out of reach of today’s inefficient ‘hybrid’ environment that relies on both paper and digital records. Electronic health records (EHRs) offer the potential for maintaining health information on individuals across all care settings and throughout their lifetimes. With proper design and monitoring, EHRs can offer improved patient care and greater protection for protected information than paper-based patient records afford.

Technology can enhance processes and add efficiencies that can lessen the impact of the shortage of knowledge workers such as medical transcriptionists and medical record technicians. Several of these technologies are described on the attached Joint Position Statement.

FEDERAL HIPAA PRIVACY AND SECURITY REGULATIONS

AHIMA, CHIA, AAMT, and MTIA are committed to strong privacy and security protections for personal health information and we were leaders in implementing the US Health Insurance Portability and Accountability Act of 1996 (HIPAA).

HIPAA was the first-ever federal privacy standards to protect patients’ personal health information took effect less than a year ago, in April 2003. They apply only to healthcare providers, payers and clearing houses (called “covered entities.”) The HIPAA security rules that will become effective in April 2005, however, also apply to the other parties (“business associates”) that have access to personally identifiable health information (such as transcription companies and other vendors). The security rules, on top of the privacy rules, have a framework that includes both civil and criminal penalties for privacy violations. These penalties can be quite large. For civil violations of the standards, the Office of Civil Rights (OCR) may impose monetary penalties up to $100 per violation, up to $25,000 per year, for each requirement or prohibition violated. Criminal penalties apply for certain actions such as knowingly obtaining protected health information in violation of the law. Criminal penalties can range up to $50,000 and one year in prison for certain offenses; up to $100,000 and up to five years in prison if the offenses are committed under "false pretenses"; and up to $250,000 and up to 10 years in prison if the offenses are committed with the intent to sell, transfer or use protected health information for commercial advantage, personal gain or malicious harm.

AHIMA, CHIA, AAMT, and MTIA have advocated full compliance with HIPAA by our members, have supported the enactment of HIPAA that imposes penalties for violations, we have provided education on how to manage outsourcing relationships. It is important to 1) continuously reinforce adherence to sound policies and procedures that comply with HIPAA, 2) improve the due diligence used in establishing and monitoring outsourcing contracts, 3) identify areas where HIPAA regulations need to be improved, and 4) punish those who violate the rules.

AHIMA has developed detailed practice briefs on HIPAA Security and Security Audits, both of which are attached.

It is important to note that the federal HIPAA rules set a floor, not a ceiling for states, so state laws that are “more stringent” than the HIPAA rules take precedence.

CALIFORNIA LAWS PROTECTING HEALTH INFORMATION

For many years, California, unlike many states, has had in place numerous comprehensive laws designed to protect the privacy of patient’s health information and to keep it from being misused. A few of these laws include:

3
The Confidentiality of Medical Information Act (Cal. Civil Code § 56 et seq.) that protects medical information held by providers, health plans and other entities.

The Lanterman-Petris-Short Act or ‘LPS” (Cal. Civil Code § 5328 et seq.) that protects medical information pertaining to treatment for mental health and developmental disabilities

Patient Access to Health Records Act (Cal. Civil Code § 123100 et seq.) that gives individuals certain rights of access to the information in their medical records

Subpoena laws (Cal. Code of Civil Procedure § 1985.3)

The Laws governing HIV test results (Cal. Health and Safety Code § 120980)

Insurance Information and Privacy Protection Act (Insurance Code § 791 et seq.) that protects personal information held by insurance companies

Personal Information Privacy law (Civil Code 1798.82 and Section 1798.29 ) requires an agency, person, or business that maintains computerized data that includes personal information owned by another to notify the owner or licensee of the information of any breach of security of the data.

RECOMMENDATIONS:

CHIA urges policy makers to consider the workforce technology, cost and legal implications of their legislative proposal. We urge lawmakers to craft regulatory solutions that enforce HIPAA and support advancements in modern healthcare information processing practices that improve the quality and cost of healthcare.

We urge increased investment in health information workforce development and implementation of new technologies to advance critical healthcare outcomes – timely accurate, accessible and secure information to support patient care. We believe it is essential that state legislatures reinforce the importance of improving information processing solutions for healthcare and not take actions that will produce unintended and detrimental consequences.

These recommendations are included on the attached Joint Position Statement issued by the American Health Information Management Association (AHIMA), the California Health Information Association (CHIA), the American Association for Medical Transcriptionists (AAMT), and the Medical Transcription Industry Alliance (MTIA).

The California Health Information Association applauds your efforts to create legislation that will further protect the privacy of consumer’s health information in California. I and my colleagues will be happy to continue to work with your staff on the important issues and strategies available to minimize the risk of breaches in patient privacy in California.