Testimony of Bryon Pickard, MBA, RHIA

President

American Health Information Management Association

to the

Committee on Oversight and Government Reform

Subcommittee on Information Policy, Census and National Archives

June 19, 2007

Introduction

Chairman Clay and members of the Subcommittee, thank you for inviting the American Health Information Management Association (AHIMA) to testify today on current privacy policies (HIPAA), and the challenge of integrating adequate privacy protections into a national health IT infrastructure. My name is Bryon Pickard, MBA, RHIA, and I am the current president of AHIMA. AHIMA is the premier association of health information management (HIM) professionals whose more than 51,000 members are dedicated to the effective management and analysis of the health data and information needed to deliver quality healthcare. 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.

In addition to my role as president of AHIMA, I am the director of operations for the Vanderbilt Medical Group Business Office at Vanderbilt University Medical Center in Nashville, Tennessee. I have also participated in privacy, confidentiality, and security design workgroups for the Vanderbilt Center for Better Health and e-Health initiatives focusing on regional and statewide health information exchange projects in Tennessee. My experience also includes leading integration, merger and audit strategies for health information systems, registration, and patient accounting applications, and I currently serve as a member of the practice management application IT advisory committee at Vanderbilt.

Today, I will be testifying on behalf of AHIMA, but will draw upon my professional experiences at Vanderbilt and the previous environments in which I worked. My testimony will focus on the public and private efforts underway to ensure the privacy of electronically transmitted health information and the effectiveness of our current laws and regulations governing the use and disclosure of such information. In addition, I will address some specific areas that are of specific interest to our profession and the reason for today's hearing:

- Expansion of privacy protections for personal health records
- Differences between HIPAA "business associates" and non-covered third-party contractors
- Protecting student health information: Health Insurance Portability and Accountability Act (HIPAA) vs. Family Educational Rights and Privacy Act (FERPA)

For almost 80 years, the HIM profession has strived to maintain the confidentiality of health records and be the patient's advocate within the healthcare system. It is with AHIMA's history and experience, along with my own, and those of the AHIMA members that I have met as an officer and director of AHIMA and the Tennessee Health Information Management Association (THIMA) that I come before you today prepared to respond to your concerns and questions on the confidentiality and security of health information.

For full disclosure, I must note that AHIMA is composed of more than 51,000 healthcare professionals, each affiliated with one of 52 state associations. In addition to a detailed academic curriculum, most AHIMA members are also certified in one or more areas of HIM, including a certification in privacy and security. AHIMA also has a foundation, the AHIMA Foundation for Research and Education (FORE), which is involved in a variety of research and academic scholarship

endeavors. It is through the reputation and experience of AHIMA members that FORE has received several grants and contracts from the Department of Health and Human Services' (HHS) Office of the National Coordinator for Health Information Technology (ONC). The grants and contracts are focused on state health information exchange analysis, the potential for fraud associated with electronic records, and subcontracts associated with the area of privacy and security. I have attached a list of those commitments to this testimony.

Mr. Chairman, the HIM professional's responsibilities are interwoven with privacy and security issues. With the advent of privacy and security rules associated with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), our profession undertook the role of addressing confidentiality and security as it relates to the electronic transmission of healthcare data—the use, access, and disclosure of health information to persons other than the individual or the individual's representative. As you are aware, the adoption of the HIPAA privacy rule was not without considerable debate and the implementation took considerable time, effort, and resources.

The expansion of confidentiality management and protection was impacted not only by HIPAA, but also by the healthcare industry's continued transformation from a paper-intensive industry to one of electronic records and transmissions. I wish I could tell you that the healthcare industry has been transformed into a fully electronic system, but, in fact, I cannot. Rather we are in the midst of what will be a long transition that will see the introduction and implementation of a standard, electronic health record, personal health records, and health information exchange networks also called Regional Health Information Organizations (RHIO) or Regional Health Information Networks (RHINs).

In working through these transitional issues, AHIMA has often partnered with the American Medical Informatics Association (AMIA) to form what we believe is a responsible approach to the healthcare industry's transformation. I want to mention this relationship because AHIMA and AMIA have produced two joint statements relevant to today's discussion:

- The AHIMA-AMIA Joint Position Statement on Health Information Confidentiality
- The AHIMA-AMIA Joint Position Statement on the Value of Personal Health Records

With so much history and experience in the protection of health information and our involvement in the current transformation of our healthcare system, it is important to state AHIMA's position related to today's topic—current privacy policies (HIPAA) and the challenge of integrating adequate privacy protections into a national health IT infrastructure. First, any organization that accesses or stores personal health information should abide by the following principles:

- Inform individuals, through clear communications, about their rights and obligations and the laws and regulations governing protection and use of personal health information (PHI).
- Notify individuals in clear language about the organization's privacy practices and their rights in cases of security breaches
- Provide individuals with a convenient, affordable mechanism to inspect, copy, or amend their identified health information/records
- Protect the confidentiality of PHI to the fullest extent prescribed under HIPAA, regardless of whether the organization is a "covered entity" as defined in HIPAA, and ensure that the

organization and its employees all comply with HIPAA, state laws, and the policies and procedures put in place to protect PHI.
- Use PHI only for legitimate purposes as defined under HIPAA or applicable laws.
- Prohibit the use of PHI for discriminatory practices, including those related to insurance coverage or employment decisions.
- Timely notification of individuals if security breaches have compromised the confidentiality of their personal health information.
- Work with appropriate law enforcement to prosecute to the maximum extent allowable by law any individual or organization who intentionally misuses PHI.
- Continue to improve processes, procedures, education, and technology so that PHI practices improve over time.

As our healthcare system evolves and becomes more interconnected, health information will flow across a range of organizational, state and potentially international boundaries through a nationwide health information network structure. As we evolve into this structure, it will be critical to follow principles covering health information when it is transferred between entities and across boundaries:

- Health information privacy protections must follow PHI no matter where it resides.
- Uniform and universal protections for PHI should apply across all jurisdictions in order to facilitate consistent understanding and compliance by those covered by such laws and the individuals whose health information is covered by such laws.

Trends Are Changing: Health Information Exchange

As members of the subcommittee are aware, a number of efforts are underway to address many of the issues we have discussed today. AHIMA, the healthcare industry, and those of us in Tennessee have spent considerable time and energy, as has Congress, exploring and developing electronic health information exchange. Whether we call such an exchange an RHIO or an HIE, the concept of moving healthcare data electronically is a critically important topic that we have now discussed for a multitude of years. We have seen various groups agonize over how to protect health information, based on where it is stored, how it might be transmitted or accessed. They have also agonized over various protections for specific types of data as behavioral health, HIV, genetic information, and so forth. The importance of specific types of data is in the eye of the beholder. Our experience has indicated to us that all health information should be treated equally—specific policy protections for specific types of data can give away its type. Yes, you can build extra layers of security requirements in your systems to protect the data but specific policy requirements can cause problems.

The HHS Agency for Health Research and Quality (AHRQ) through its subcontractor RTI is finishing a research project, Health Information Security and Privacy Collaboration (HISPC), that covered the privacy and security environment of some 34 states and territories. The final report from this project is due shortly and separate reports have been generated by the 34 states and territories, indicating where laws, regulations, and business practices related to privacy and security, potentially stand as barriers to the implementation of standard Electronic Health Records (EHR) and the exchange of electronic health information. Already, many of the groups that participated in this effort at the state level, have indicated that they have or will undertake additional efforts to address and resolve these barriers on a state level. At the same time, these same groups have indicated that such projects may take multiple

years. For instance, the group involved in Florida indicated that there are more than 60 chapters of state law that need to be addressed to arrive at a uniform set of code to address health information privacy in that state. While we would like to see uniformity at the state, regional, and national levels, we must recognize just what a large project this will be.

ONC, based on preliminary reports from the AHRQ effort, and the State HIE Best Practice Project (that AHIMA/FORE coordinated) has engaged the National Governors Association (NGA) to look at the potential to design uniform state laws or regulations that might bring us the uniformity and consistency needed for a national health information exchange system or network. The NGA effort began this last January. Included in the effort is a committee addressing the protection of health information. The NGA is aware that there are several more formal efforts that have already begun in the states by some individual governors. It is unclear if the governors themselves are trying to keep their individual efforts open to national uniformity as they move forward.

Secretary Leavitt initiated the American Health Information Community (AHIC) in 2005. While privacy was not an initial focus, the Community quickly identified the need to address confidentiality issues in their efforts, and a workgroup on confidentiality, privacy, and security was formed. This group has addressed some areas of identity proofing and the need to protect PHI wherever it might reside, but it also has indicated that there are many more efforts needed including the authentication of individuals involved in health information.

As the Community has addressed standards, and the need for confidentiality, it has also made recommendations for how standards may be affected by privacy and the need for certification of health information technology products that include basic security to facilitate confidentiality. As a result of this effort, the Health Information Technology Standards Panel (HITSP) is looking at confidentiality and privacy standards, and the Commission for Certification of Health Information Technology (CCHIT) is looking to establish certification criteria to identify technology that meets the principles established by the Community and HHS.

As noted, the HHS National Committee on Vital and Health Statistics (NCVHS) has had health information confidentiality as a focus ever since NCVHS was designated as the advisory committee to oversee HIPAA. In recent years the NCHVS Privacy and Confidentiality Subcommittee has concentrated on post-HIPAA privacy and security issues as well as confidentiality as it applies to a nationwide health information network and personal health records. While AHIMA does not support all the recommendations of the NCVHS, we have been very pleased with the work and testimony that the committee has undertaken, and as noted we specifically would point out their efforts on HIPAA versus FERPA.

As members of the committee are aware, the House has passed legislation related to nondiscrimination on the basis of genetic information (HR 493, the "Genetic Information Nondiscrimination Act"). This legislation is now on "hold" in the Senate. As I have noted, AHIMA believes that nondiscrimination should apply to all health information, not just genetic and we would hope that Congress would consider such an approach.

Our members, especially those who fill the role of privacy officers (required by HIPAA) are noting that the issue of privacy for them is moving beyond just healthcare. With the banking and finance

industries becoming more involved in privacy we see that we must soon address the protection of an individual's information uniformly whether it is financial or healthcare. This is an issue that Congress will need to follow as we see more movement and change in healthcare.

As I have mentioned, we also see a need for consumer education. Education needs to address confidentiality and security as well as health information technology and the new environment. It is only with consumer trust that we can build a national infrastructure and adopt or modify laws to facilitate such an exchange.

I have also alluded to that fact that AHIMA and its members are very involved in the area of confidentiality and security. Many of our members are involved in efforts surrounding the PHR, HIE, and protections for health records whether they are paper, electronic, or hybrid form. While it would be wonderful to see one concerted effort, we know from experience that there is a tremendous amount of work that needs to be done because of our federal foundation and approach to legislation and regulation, as well as the evolution that is going on in health information technology and management.

Expansion of Privacy Protection for PHRs

AHIMA has long called for consumer-based personal health records in addition to provider-based electronic health records. This goes back even before the creation of jump-drives and Web-based portals. It has been our contention that consumers should have a copy of their medical record, track their current health status, and have an overall healthcare awareness. We have never endorsed a method or a PHR product. We have just endorsed that consumers should use a PHR—whether in paper or electronic form.

To spread the word on the importance of PHRs, AHIMA embarked upon a consumer-education campaign. This campaign combined the use of a consumer Web site, www.myPHR.com, with nationwide public speaking engagements by AHIMA members in each and every state.

The Web site is a tool that helps visitors some important questions about personal health records:

- Why start a PHR?
- What should your PHR contain?
- What are the steps to be taken to create a PHR?
- Are there different ways to keep your PHR?

In addition, the site provides a free health record form that will help consumers start their own PHRs.

As our public-education campaign continues, so do personal health record developments. Although there is no single model of a personal health record, there are some important concepts that should apply to any PHR.

Today, AHIMA and others in the industry are working hard on interoperable and data standards that will ensure that any electronic PHR is capable of being interoperable with the standard EHR and other electronic records. Currently, AHIMA is leading an effort to ensure the interoperability of the PHR with the Health Level Seven (HL7) standard electronic health record. We expect to see

a new HL7 standard in the not too distant future. AHIMA defines the PHR as "…an electronic, universally available, lifelong resource of health information needed by individuals to make health decisions. Individuals own and manage the information in the PHR, which comes from healthcare providers and the individual. The PHR is maintained in a secure and private environment, with the individual determining rights of access. The PHR is separate from and does not replace the legal record of any provider."

As I indicated, AHIMA believes that protection should follow the personal health information no matter where it might be stored or transferred. This clearly extends to PHRs, which can be stored or offered by a variety of different vendors or operators. Some of these vendors are covered by HIPAA, because they have some healthcare claims function that has made them a HIPAA-covered entity. A few vendors may be covered by state law, but it must be noted that neither HIPAA nor most state laws considered PHRs. The industry is moving that quickly.

Clearly today, PHRs offered by non-HIPAA-covered entities have no protection unless there is state legislation that specifically addresses the issue. Even if state legislation exists, there is concern if the PHR operator is in one state, and the consumer is in another, which law applies and/or prevails. In line with consumer concerns related to discrimination and misuse of personal health information, we recommend that uniform laws be written to cover the misuse of personal health information regardless of where it resides or is transmitted – this would then include the personal health record.

A concern with the information in a PHR relates to who has access and can use the information beyond the individual. As I noted, there are a variety of models of PHRs offered HIPAA covered entities and others. The question is what access and responsibilities should govern the operator or vendor of the PHR. Some health plans have indicated that they have the right to access and use PHRs they operate under the "Treatment, Payment, and Healthcare Operations (TPO) of HIPAA. We think such access for a PHR should be questioned. The first word in PHR is "personal" and it makes sense that the individual provide an additional authorization for any access or use of this PHR record set outside of the individual's own use. If the individual cannot control the access and use to their own PHR, their ability to trust and ensure the appropriate use of their personal information will be eroded. This is especially true when the PHR is in the hands of a third party where there is a concern about potential misuse or discrimination.

Our recommendation, therefore, not only extends to protection against the discrimination and misuse of PHR information, but also for establishing a requirement that any access or use be governed by a separate authorization unless otherwise required by law. In addition, except for PHRs offered by healthcare providers, we believe that individuals (in this case usually subscribers or employees) should be given the right to opt-out of a PHR being built for them or their affected family members. This would mean that no PHR would be populated even with claims data.

While we have some concerns for how some PHRs are populated with claims data, we are pleased to see healthcare providers, health plans, employers, and other types of organizations take steps to make such records available for individuals and for healthcare providers when such data is needed. Even so, the consumer must be fully aware of how the record is populated and how it can be accessed and used. Not only used by themselves, but by their healthcare providers and by the operators of the PHR. If

awareness is not a component, PHRs will fall into misuse, which itself could endanger the health of the individual.

Difference Between Business Associates and Third Party Non-Covered Entities

The privacy officer members of AHIMA have often cited the business associate requirement as one of the more difficult aspects of HIPAA to manage. This is especially true when you have a small provider contracted with a very large subcontractor who sets the tone of the relationship. Business associates in the realms of privacy would be subcontractors of HIPAA-covered entities, which, as I have already noted, are not all the parties that could be involved with personal health information. Under HIPAA, the covered entity would identify the HIPAA responsibilities to the subcontractor or business associate and the business associate would then be responsible for compliance. If a HIPAA entity discovered that a business associate was not in compliance with HIPAA then it would take corrective action or cancel the contract. The contracts also become difficult to manage when the covered entity's subcontractor itself subcontracts out to complete the work requirements in the contract. As we have seen in some cases, this subcontractor list can extend to multiple parties.

Once again, situations such as these show the need for the confidentiality and security protections to follow the data no matter where it resides or is transferred. The entity holding the identifiable personal health information should be responsible for its safekeeping. The Confidentiality, Privacy, and Security (CPS) Workgroup of the HHS advisory body AHIC last week made a similar recommendation to the Secretary. The CPS recommended:

- *"All persons and entities, excluding consumers, that participate directly in, or comprise, an electronic health information exchange network, through which individually identifiable health information is stored, compiled, transmitted, modified, or accessed should be required to meet enforceable privacy and security criteria at least equivalent to any relevant HIPAA requirements (45 CFR Parts 160 and 164)."*

- *"Furthermore, any person or entity that functions as a Business Associate (as described in 45 CFR §160.103) and participates directly in, or comprises, an electronic health information exchange network should be required to meet enforceable privacy and security criteria at least equivalent to any relevant HIPAA requirements, independent of those established by contractual arrangements (such as a* Business Associate Agreement *as provided for in HIPAA)."*

AHIMA's immediate past president, Jill Callahan Dennis, JD, RHIA, is a member of the CPS workgroup and we believe these recommendations make a lot of sense. The world is far too complicated to be able to use a "business associate" approach especially when we are discussing electronic health exchange among a variety of different entities. Again, let the protections follow the data, and make all parties responsible for confidentiality.

Employer Requests for Information

Another important issue in the current personal health information landscape concerns employer requests for health information. If you have seen some of the consumer polls, you know that consumers have indicated less concern for where their health information resides. Why? Consumers

want their health information to benefit themselves, their families, and their communities. However, what the polls have consistently showed is that consumers fear that their information may used against them for discriminatory purposes by their employer, potential employer, and/or insurers. Eliminating this fear of discrimination is crucial to creating trust in our system and with moving forward with electronic health information exchange. If we can secure data and create trust then we will have an easier time having the data available for a variety of important population health needs as quality measurement, public health surveillance, biosurveillance, and health research.

There are legitimate needs for employers to have some health information about their employees or potential employees, just as there are a few reasons why some insurers need some health information concerning their insured or potential insured. In this instance, I am talking about access to information outside the claims process. We - and I think this is a government role - need to define the misuse of data and the legitimate reasons for why an employer might require access to personal health information or request information from an employee or potential employee. It is important to define what constitutes health information discrimination versus the legitimate needs for information. Then, if discrimination exists, it should be punished.

It is the government's role to establish a means of punishing those who discriminate or misuse data. Misuse could be the intentional and unwarranted access to, use of, or distribution of an individual's personal health information. There are some laws on the books, including those passed by Congress in 1997, but there have been very few prosecutions. If the public begins to see that the healthcare industry and government are active in this area, it will likely create a greater trust in the system by showing the public that misuse of data has serious ramifications.

Strong "misuse of PHI rules" would also allow the industry and government to prosecute the intentional breeches of information that we have seen reported in the media. I do not mean to suggest that all of the potential breaches are intentional or result in a loss of protection. But our industry does need to be held accountable for the security of health information. Let us send a message to anyone who desires to breach the confidentiality of healthcare information that they will be punished. Let the protection follow the data and let's punish those who misuse healthcare data or discriminate on the basis of healthcare data. If we do not, consumers will not have trust in our development of EHRs, our establishment of EHI, and access to secondary health information that will better society.

Student Protections

Another important area of consideration is protecting the healthcare data of students. Student healthcare data has two masters, the HIPAA privacy rule and FERPA. Over the past several years, the NCVHS Subcommittee on Confidentiality and Privacy has held several hearings that have highlighted the problems created by having these two laws overlap.

Gone is the day when the school nurse took your temperature and put you on a cot until it was time to go home. Today's school nurses are dealing with students on a variety of drug regimens, some even sporting infusion pumps. Disease outbreaks require that school districts have immunization records. The schools and their nurses should not have to beg parents and family physicians for records. High school coaches need to have a clear and accurate health picture of the players on their teams to take precautions against the child with a heart condition collapsing on the field. It is a difficult balance.

Even though this information is needed to protect against disaster, it should not be available to everyone in the school or in the locker room. FERPA was not designed to provide the protections that Congress and the states have seen as necessary for health information.

Administration of both rules becomes even more difficult for schools such as Vanderbilt. The rules reside side-by-side. Again, we owe it to our citizens to protect the confidentiality of their health information. We suggest that the Congress look at the testimony and recommendations made by the NCVHS with regard to FERPA and HIPAA issues and seek to extend, at a minimum, HIPAA protections to all healthcare data, so there is no question about which of the two laws prevails when discussing healthcare data.

Conclusion

Currently the transformation in healthcare is occurring at a pace unheard of in the industry, and yet some would say it should move even faster. The transformation in healthcare is not just converting healthcare data from paper to electronic, but it is also transforming the business processes and uses of information required in such a metamorphosis. In addition to this conversion we have even more consumer involvement, and rightly so, calling for rigid confidentiality and security assurances that will protect individuals against discrimination and the misuse of their healthcare information. That's a big order, and as I have alluded to, this transformation and culture changes, it is not happening overnight, but rather will take many years. In the meantime we now find ourselves in the midst of change and in an environment that is neither all paper nor electronic. We also find ourselves in an environment never anticipated by myriad existing federal and state laws and regulations that impact our abilities to make the conversion and preserve the needed confidentiality and security practices we have addressed this afternoon.

The industry is in a major transition where different health information exchange models are being discussed for a multitude of environments. While we might desire a simple answer as soon as possible, this will not be the case. Once again, we must suggest that the healthcare industry and government provide protections that will permit a variety of models and the time to approach more specific rules and regulation. As we move forward we must ensure that personal health information is protected wherever it might reside. We must ensure that individuals are protected against the misuse of their health information for discriminatory and other nefarious purposes. And finally, we must ensure that individuals continue to have a right to access to their own healthcare information

In addition to our efforts to make laws, regulations, and practices standard, there is similarly a need to address just how health information technology impacts concerns for privacy. We in the HIM profession believe that new information technology will permit even better security and confidentiality, if the principles and processes surrounding such technology are applied intelligently. But, we have a major need for educating and an understanding of EHRs, PHRs, information exchange.

History has shown that there is no silver bullet that will solve everything, but while goals and objectives and even principles can be stated, a detailed map of milestones is very difficult to achieve in our system of government and under our healthcare model. I can assure the committee that many are working on this effort and our goals are becoming more uniform as we move forward.

Over the years, some in Congress have made consistent efforts to legislate in the privacy area. It has been a difficult undertaking to say the least. As the AHIC, NCVHS, and others discuss and provide recommendations in the privacy and security area, Congress can also begin to look at some very important issues:

- The need to ensure that confidentiality protections follow the information no matter where it resides or is transferred.
- Comprehensive nondiscrimination legislation that has harsh penalties for the misuse and illegal requests for health information.
- The need to prosecute those who break the law.
- The need to penalize those entities whose confidentiality and security processes and technologies do not comply with the level of confidentiality protection required by law.
- The need to eliminate the conflicts between HIPAA v FERPA.
- Conscientious review of proposed laws to identify barriers that may arise that would impede deployment of health information technology products, expansion of health information exchange, and critical uses of health information—as for quality reporting, biosurveillance, and public health.

Mr. Chairman and members of the subcommittee, I hope that my testimony has given you insight into the aspects of healthcare confidentiality and security that you are seeking and that my recommendation will provide you with guidance as you address the many thorny questions facing our community. I stand ready to answer any further questions or concerns you might have, and as president of AHIMA, I similarly make available to you the resources of our staff to assist in any way possible.

Contact information.

Bryon Pickard, MBA, RHIA
Director of Operations
Vanderbilt Medical Group
2146 Belcourt Ave.
Nashville, TN 37212
(615) 936-2000

Don Asmonga, MBA
Director of Government Relations
AHIMA
1730 M Street, NW, Suite 502
Washington, DC 20036
(202) 659-9440

Dan Rode, MBA, FHFMA
VP, Policy & Government Relations
AHIMA
1730 M Street, NW, Suite 502
Washington, DC 20036
(202) 659-9440

Craig May
Director of Public Relations
AHIMA
233 N. Michigan Ave.
21st Fl.
Chicago, IL 60601-5800
(312) 233-1100

Statement on Health Information Confidentiality
A Joint Position Statement
by
American Medical Informatics Association
American Health Information Management Association
July 2006

The American Medical Informatics Association (AMIA) and the American Health Information Management Association (AHIMA) have a long history of working to protect the confidentiality of individuals' health information and to promote fair information practices. Public confidence that privacy will be protected and that identifiable information will be used only for purposes authorized by the individual, or otherwise permitted by law are essential to ensuring trust in a nationwide health information network (NHIN that facilitates sharing of personal health information (PHI). As the United States progresses from a paper-based system of health records to an electronic environment, AMIA and AHIMA believe that the following principles should be incorporated in all rules, regulations, or laws pertaining to PHI.

Any organization that accesses or stores PHI should abide by the following principles. The organization should:

- Inform individuals, through clear communications, about their rights and obligations and the laws and regulations governing protection and use of PHI.
- Notify individuals in clear language about the organization's privacy practices and their rights in cases of breaches
- Provide individuals with a convenient, affordable mechanism to inspect, copy, or amend their identified health information/records
- Protect the confidentiality of PHI to the fullest extent prescribed under HIPAA, regardless of whether the organization is a "covered entity" as defined in HIPAA, and ensure that the organization and its employees all comply with HIPAA, state laws, and the policies and procedures put in place to protect PHI.
- Use PHI only for legitimate purposes as defined under HIPAA or applicable laws.
- Prohibit the use of PHI for discriminatory practices, including those related to insurance coverage or employment decisions
- Timely notification of individuals if security breaches have compromised the confidentiality of their personal health information.
- Work with appropriate law enforcement to prosecute to the maximum extent allowable by law any individual or organization who intentionally misuses PHI
- Continue to improve processes, procedures, education, and technology so that PHI practices improve over time.

Furthermore, because PHI is expected to flow across organizational boundaries through the NHIN, it is important that the following principles covering information when it is transferred from one entity to another also apply:

- Health information privacy protections must follow PHI no matter where it resides

- Uniform and universal protections for PHI should apply across all jurisdictions in order to facilitate consistent understanding by those covered by such laws and the individuals whose health information is covered by such laws.

About AMIA
The American Medical Informatics Association (AMIA) is an organization of 3,500 health professionals committed to informatics who are leaders shaping the future of health information technology and its application in the United States and 41 other nations. AMIA is dedicated to the development and application of informatics in support of patient care, teaching, research, and health care administration and public policy. www.amia.org

About AHIMA
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

7-31-2006

The Value of Personal Health Records
A Joint Position Statement for Consumers of Health Care
by
American Health Information Management Association
American Medical Informatics Association
February 2007

Position

The American Health Information Management Association (AHIMA) and the American Medical Informatics Association (AMIA) advocate empowering individuals to manage their healthcare through the use of a personal health record (PHR). The PHR is a tool for collecting, tracking, and sharing important, up-to-date information about an individual's health or the health of someone in their care. Using a PHR will help people make better health decisions and improves quality of care by allowing them to access and use information needed to communicate effectively with others about their healthcare.

Basic Principles

- Every person is ultimately responsible for making decisions about his or her health.
- Every person should have access to his or her complete health information. Ideally it should be consolidated in a comprehensive record.
- Information in the PHR should be understandable to the individual.
- Information in the PHR should be accurate, reliable, and complete.
- Integration of PHRs with EHRs of providers allows data and secure communication to be shared between a consumer and his or her healthcare team.
- Every person should have control over how their PHR information is accessed, used and disclosed. All secondary uses of PHR data must be disclosed to the consumer, with an option to opt-out, except as required by law.
- PHR products should be certified by CCHIT to comply with data standards, include a minimum data set, identify each data's source, and meet security criteria consistent with HIPAA
- The operator[1] of a PHR must be accountable to the individual for unauthorized use or disclosure of personal health information. The consumers should be notified immediately of breaches in security that could lead to disclosure of personal health information.
- A PHR may be separate from and does not normally replace the legal medical record of any provider.
- Privacy protection of PHR data should follow the data. PHR data must not be used in any discriminatory practices.

[1] An "operator" could be a healthcare provider, health plan, commercial supplier, government agency, employer, union, fraternal order, and so forth.

Questions and Answers

Why should everyone have a PHR? We believe that all individuals should be able to readily access, understand, and use their personal health information. A PHR allows individuals to be more active partners in their healthcare, and gives them up-to-date information when and where they need it. A PHR provides a single, detailed and comprehensive profile of a person's health status and healthcare activity. It facilitates informed decisions about the care of the individual. It may also reduce duplicate procedures or processes – such as repeated lab tests and x-rays – saving time and money. A PHR helps people prepare for appointments, facilitates care in emergency situations, and helps track health changes.

What media should you use for a PHR? We encourage individuals to begin tracking their health information in whatever format works best for them, even if the choice is paper. We recommend that individuals use an electronic media to facilitate a timely, accurate, and secure exchange of information across healthcare institutions and providers. PHR information should always be stored in a secure manner just as you would store other confidential personal information such as financial information.

How can an individual choose a PHR supplier? Individuals can create their own PHR, or may be offered one by a variety of sources, such as a healthcare provider, insurer, employer or a commercial supplier of PHRs. Each supplier has different policies and practices regarding how they may use data they store for the individual. Study the policies and procedures carefully to make sure you understand how your personal health information will be used and protected. Policies to look for include privacy and security; the ability of the individual, or those they authorize, to access their information; and control over accessibility by others. If the PHR contains the same information that the doctor has seen, it has more usefulness for tracking purposes than information from insurance forms. For example, insurance claims information may list the diagnosis or medication but not the details (for example, actual blood pressure reading or dose of the medication taken).

What should a PHR contain? Broader than a medical record, the PHR should contain any information relevant to an individual's health. In addition to medical information such as test results and treatments, a PHR may include diet and exercise logs or a list of over-the-counter medications. A PHR should contain the following information:

- Personal identification, including name and birth date
- People to contact in case of emergency
- Names, addresses, and phone numbers of your physicians, dentists, and specialists
- Health insurance information
- Living wills, advance directives, or medical power of attorney
- Organ donor authorization
- A list and dates of significant illnesses and surgical procedures
- Current medications and dosages
- Immunizations and their dates
- Allergies or sensitivities to drugs or materials, such as latex
- Important events, dates, and hereditary conditions in your family history
- Results from a recent physical examination
- Opinions of specialists
- Important tests results; eye and dental records
- Correspondence between an individual and his or her provider(s)
- Current educational materials (or appropriate Web links) relating to one's health

Where individuals should begin: A good place to begin is with a visit to www.myPHR.com (a site provided as a free public service by AHIMA) for further information on creating and managing a PHR. We suggest that people find out if their healthcare providers, employer, insurers, or another individual or organization offers a PHR. If an individual needs to obtain copies of medical records themselves, they can contact doctors' offices or each facility where they have received treatment.

Each person can create a PHR at his or her own pace, perhaps starting with the next medical visit. The important thing is to get started.

Note: Because the use of personal health records is an issue of importance to both organizations, AHIMA and AMIA collaborated on the development of this joint position statement.

About AHIMA
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

About AMIA
The American Medical Informatics Association (AMIA) is an organization of 3,500 health professionals committed to informatics who are leaders shaping the future of health information technology and its application in the United States and 41 other nations. AMIA is dedicated to the development and application of informatics in support of patient care, teaching, research, and health care administration and public policy. www.amia.org

2-1-2007

Foundation of Research and Education/AHIMA Sponsored Programs, Research Contracts and Grants* January 1, 2006 to April 23, 2007			
A. Active Projects 2007; B. Proposals Pending 2007; C. Projects Funded and Completed 2006 and 2007; D. Proposals without Funding, Rejected, or on Hold for Other Reasons			
A. Active Projects 2007			
Federal Contract	ONC—State Level Health Information Exchange Consensus Project	Office of the National Coordinator (ONC)	Primary Staff Involvement: Sue Fiorio, Aleta Harris, Linda Kloss, Eileen Murray, Carol Nielsen, Theresa Reynolds
The purpose of this contract is to build on and extend the work produced to date by the Foundation of Research and Education (FORE) on emerging best practices and guidance for state level health information exchange initiatives (HIEs). These organizations are evolving very rapidly and the lessons learned must be documented, studied, and made available to all state level entities and other interested stakeholders. This contract will produce research-based technical work products to expand the body of knowledge of emerging best practices. It is expected that these will help not only state level HIE initiatives, but also regional health information exchange initiatives, state governmental e-Health programs and others who are working to advance care transformation through health information.			
Value of Total Contract: $793,785.00			
Federal Professional Services Contract	#200-2006-M-18081: Training for Coders for Morbidity and Mortality: ICD-10 Curricula	CDC: National Center for Health Statistics	Primary Staff Involvement: Kathy Giannangelo
This project involves implementing, piloting, and evaluating the first phase of the International Training and Certification Program for ICD-10 Mortality and Morbidity Coders. The purpose of the project is to expand on the work already accomplished by the Joint Collaboration to pilot the processes for testing and certification of practicing ICD coders and newly trained coders and for the recognition of ICD trainers and educators and to evaluate the strengths and weaknesses of the processes. The project also will perform outreach to coders and trainers in order to inform them of the availability and benefits of the international program.			
Value of Total Contract: $20,000			
Subcontract from RTI for Professional Services Funding Primary Source is AHRQ	Contract to Develop Model Anti-Fraud Requirements for Electronic Health Records	HHS/AHRQ	Primary Staff Involvement: Michelle Dougherty, Don Mon, Harry Rhodes
The RTI research team has previous experience identifying fraudulent or otherwise suspicious activity in large datasets and recommends an iterative two-pronged approach for this task, which includes the use of scoring algorithms and anomaly detection. Known patterns of fraudulent behavior can be characterized and modeled using supervised learning or rule induction models. The resulting scoring algorithms can be used to screen transactions for potentially fraudulent or otherwise suspicious activity. Unsupervised learning strategies, on the other hand, can be used to identify unusual or anomalous activity worthy of additional review and follow-up. Fraudulent behavior identified through the use of anomaly detection can then be modeled and added to the array of scoring algorithms used to screen additional data for patterns suggestive of fraud or other suspicious activity.			
Value of Total Contract: $115,326.00			
Contract	Center for Aging Services Technology: Development of a Framework for Continuity of Care Document (CCD) Functional Status and Wellness Content	Center for Aging Services Technology—a program of the American Association of	Primary Staff Involvement: Jill Burrington-Brown, Rita Scichilone

	RE ID #: 35501	Homes and Services for the Aging	
AHIMA will assist in the establishment of stakeholder work groups to advance health information technology and terminology standards related to functional status assessment and advocacy for electronic health record use for wellness measurement and consumer empowerment through the use of personal health records.			
Value of Total Contract: $54,600.00			
Service Contract	SNOMED:ICD-9-CM Map Validation Process – Phase II	National Library of Medicine	Primary Staff Involvement: Jill Bonnart, Susan Fenton, Kathy Giannangelo, Karen Kostick, Rita Scichilone
Note: this project is funded but the actual task is still in the proposal phase. This is a draft of the tasks that were submitted. The goal of this phase of the map validation project is to produce small subsets of the SNOMED:ICD-9-CM reimbursement use case map in a timely fashion for testing and use by the industry. Given that this is a reimbursement use case map; this phase will focus on the most frequent conditions and diagnoses as determined by the National Center for Health Statistics via their National Hospital Discharge Data Set and National Ambulatory Care Data Set. It is thought that these will be more representative of diagnoses submitted to all payors rather than utilizing CMS data which, of course, is limited to CMS claims.			
Value of Total Contract: $13,999.62 carried over from the base year plus $50,000 from Option Year 1--grand total of $63,999.62 for use in Option Year 2.			
B. Proposals Pending			
Federal Grant	AHRQ—Ambulatory Safety and Quality: Enabling Patient-Centered Care through Health IT: Effects of Patient-Centric Care Management Technology: A Randomized Trial	HHS: AHRQ RFA-HS-07-007	FORE Subcontract: Jill Burrington-Brown, Susan Fenton, Carol Nielsen
Letter of Intent: January 19, 2007; Proposal February 15 Prime: Univ. of Central Florida, Dr. Thomas Wan, PI The proposed research focuses on a demonstration of patient-centric care technology to improve medication management, utilizing the PHR as a facilitator for improved patient-provider communication. The patient-centric care technology demonstration project will assess and address the use of PHR health Information Technology (IT) as a facilitator for improving ambulatory patient safety and quality, identify the systemic barriers to health IT adoption for older, minority and underserved populations, improving patient health outcomes and asses patient–clinician satisfaction. Additionally, the PHR is a vehicle for developing a process for obtaining and documenting a complete list of current patient medications at each office visit, reducing medication errors by deescalating Adverse Drug Events (ADE) and Sentinel Events(SE) from medications, improving perceptions of patient-clinician communication, and measuring healthcare outcomes, specifically inappropriate use of healthcare resources.			
Totals	Yr. 1 $50, 745.00	Yr. 2 $19,221.00	Yrs. 3 $24,743.00	Total Direct & IDC over 3 years
Federal Grant	AHRQ—Ambulatory Safety and Quality: Enabling Patient-Centered Care through Health IT: Performance Measure Variation: Data Elements, Collection, and Outcomes		RFA-HS-07-002	Susan Fenton, Crystal Kallem, Eileen Murray, Carol Nielsen
Letter of Intent: January 19, 2007		Submitted on 2/14/2007	Anticipated Star Date: July, 2007	Prime: Dr. Jennifer Garvin, VA Philadelphia
Contract	Consultation on key questions concerning the	Language and Computing	Primary Staff Involvement: Rita Scichilone	

	E&M rules and review of possible interpretations.		
Language and Computing (L&C) is building a coding for billing NLP application that initially focuses on E&M coding. As part of the process, L&C must ensure that it follows applicable rules according to widely accepted interpretations. Interpretation of rules is a major variable for two reasons. First, the rules published by the payors, including Medicare, are extremely imprecise. Second, there are intermediates in the payment process called "carriers" for each region of the country that are responsible for implementation. These "carriers" are able to apply their own interpretations of the rules. The best recourse for a vendor in our situation is to develop a consulting relationship with an organization that has broad knowledge of the issues raised by interpretation of rules. AHIMA is the organization in the best position to help L&C in this manner. Staying abreast of coding issues is one of the roles they play for the provider community. It is a respected organization by both providers and payors. Ultimately, AHIMA will be involved in an independent evaluation of our tools. Thus, they are an ideal source for consulting about interpretation of coding for billing rules.			
Value of Total Contract: $9600 depending upon number of hours billed			
Federal Grant	AHRQ Small Conference Grant Program: Solutions to Accelerate SNOMED CT ® Implementation in Electronic Health Record Systems	HHS: AHRQ	Primary Staff Involvement: Susan Fenton, Kathy Giannangelo
The Foundation of Research and Education (FORE) of the American Health Information Management Association (AHIMA) will hold a cross industry national conference to identify solutions to expand and accelerate the adoption and implementation of SNOMED CT® in Electronic Health Record (EHR) systems. This conference will convene approximately 125 representatives from various stakeholder organizations who can determine the enablers and barriers to adoption and use of SNOMED CT in the short and long term. The participants will describe the business case for a reference terminology and develop recommendations for an integrated strategy for the use of the SNOMED CT data standard. Participants will contribute to the development of a white paper and other supporting documentation that will describe a nationwide strategy for aligning vendor and end user SNOMED CT implementation efforts so they converge and can serve as a foundation for health information exchange.			
Value of Total Grant Application: $46,182.59			
C. Projects Completed in 2006 and 2007			
Federal Contract	HHSP23320064105 EC: RHIO Develop Consensus Best Practices for State Level Regional Health Information Organizations—Initial Contract March to August, 2006	Office of the National Coordinator (ONC)	Primary Staff Involvement: Linda Kloss, Don Mon, Eileen Murray, Harry Rhodes
The purpose of the project was to gather information from existing state-level RHIOs to determine successful governance, legal, financial and operational characteristics, to develop consensus on guidance for developing state-level HIE initiatives, and to widely disseminate these findings. The research was guided by a Steering Committee of leaders from the state level RHIOs that were studied and a panel of national experts who served as Technical Advisors. They identified these three targeted areas, the interaction with federal activities, financial sustainability through HIE, and the role of payers, as critical areas for further inquiry.			
Value of Total Contract: $489,745.00			
Subcontract from Research Triangle Institute—Federal Flow-Through	Privacy and Security Solutions for Interoperable Health Information Exchange	HHS/AHRQ	Primary Staff Involvement: Susan Fenton, Don Mon, Harry Rhodes
The American Health Information Management Association (AHIMA) developed an assessment tool evaluating perceived barriers in state laws and business practices that pose interoperability challenges and hinder the free flow of information among all stakeholders involved in interoperable health information exchange and identify “best” practices for overcoming interoperability barriers.			

Value of Total Contract: $63,345.00			
Subcontract	National Conference On Health Care Data Collection and Reporting	AHRQ	Primary Staff Involvement: Crystal Kallem, Don Mon, Alison Viola
The Foundation of Research and Education (FORE) of the American Health Information Management Association (AHIMA) and the Medical Group Management Association Center for Research (MGMA CFR) have partnered with the Agency for Healthcare Research and Quality to conduct a national conference on heath care data collection and reporting. This invitational conference will convene approximately 50 persons from various stakeholder organizations that can contribute to the development of a set of recommendations for effectively coordinating various performance measurement initiatives to maximize value and minimize data collection burden and expense for health care providers. Participants will contribute to the development of multiple articles and papers that will describe a national strategy for developing standard methodologies in health care performance measurement, data collection and reporting.			
Value of Total Contract: $21,525.00			
Federal Contract	HHSP23320064105 EC: RHIO Develop Consensus Best Practices for State Level Regional Health Information Organizations—Second Extension	Office of the National Coordinator (ONC)	Primary Staff Involvement: Crystal Kallem, Linda Kloss, Don Mon, Eileen Murray, Harry Rhodes
This project will study three specific aspects of the operation of state-level Regional Health Information Organizations (RHIOs): their interaction with federal activities for health care and information technology, health information exchange (HIE) projects that have achieved financial sustainability and the role of public payers on state-level HIE.			
Value of Total Contract: $199,890.00			
Federal Contract	HHSP23320064105 EC: RHIO Develop Consensus Best Practices for State Level Regional Health Information Organizations—Third Extension	Office of the National Coordinator (ONC)	Primary Staff Involvement: Linda Kloss, Eileen Murray

The purpose of this contract extension is to establish and support a dynamic process for continuing to build the body of knowledge about the best practices of state-level health information exchange (HIE) initiatives.

This contract extension will put in place the structure and processes to study and document best industry practices as they continue to evolve in these and other organizations. In this way, the *Workbook* and related resource materials will be a dynamic reflection of dynamic organizations. The specific goals are as follows:

- Track the evolving practices of selected HIE organizations in the areas of governance, financing, health information exchange, and technology and incorporate these into an up to date *Workbook.*
- Host quarterly roundtables to seek input to strategic issues that reflect barriers or opportunities, changing market conditions, or new lessons learned and prepare reports of these deliberations.
- Capture characteristics and competencies of the evolving models for state-level HIEs
- Ensure that findings are communicated to all interested state-level HIE organizations and are available through the AHRQ HIT Resource Center, to the NGA State Alliance for e-Health, the National Conference of State Legislatures and to other public domain resource centers working to advance health IT.
- Serve as a point of contact to represent the state-level HIE perspective

Value of Total Contract: $139,958.63