# Testimony of Barbara Siegel, MS, RHIT, FAHIMA
# on behalf of the American Health Information Management Association
# to the
# Ad Hoc Workgroup for Secondary Uses of Health Data of the
# National Committee on Vital and Health Statistics
# August 2, 2007

## Opening Comments

Chairman Cohn, members of the National Committee on Vital and Health Statistics (NCVHS) Ad Hoc Workgroup for Secondary Uses of Health Data, ladies and gentlemen good afternoon. I would like to thank the workgroup and its consultant Margaret Amatayakul for the opportunity to provide input into this very timely and important discussion surrounding the development and use of secondary data, and the confidentiality and security functions surrounding the release and use of such data.

I am Barbara Siegel, director of health information at Hackensack University Medical Center (HUMC) in northern New Jersey. HUMC is a 680-bed tertiary care, teaching facility, which participates in many data reporting initiatives. Included in these initiatives are the Centers for Medicare and Medicaid Services (CMS) quality demonstration with Premier, the Institute for Healthcare Improvement Pursuing Perfection grant, and the State of New Jersey, as well as many other requests from a variety of sources seeking secondary data.

Today, I speak to you as a department director whose responsibilities include leadership over 175 employees as well as participation in organizational process improvement initiatives including revenue cycle, performance improvement, information technology, staff development and public reporting. I also speak to you today as a representative of the over 51,000 health information management (HIM) professionals who make up the membership of the American Health Information Management Association (AHIMA),[i] from whom you sought information on the collection of data for quality measurement and other secondary data purposes.

It is HIM professionals who manage the many tasks associated with gathering and analyzing the data which makes up an individual's primary record. These professionals are also responsible for disseminating data for a variety of secondary functions including quality measurement, public health or biosurveillance, research, and a myriad of administrative and operations reporting requirements.

## Internal Policy and Practice for External Reporting of Secondary Data

In 2004, I provided the NCVHS Workgroup on Quality with a brief description of HUMC's quality reporting activities and staffing requirements. In June of this year, the AHIMA and the Medical Group Management Association (MGMA) provided a report to the Workgroup on Quality, and in part provided an update on the administrative costs HUMC is now experiencing. This now includes a 72 percent increase in costs due to an increase in demand for data and a resulting increase in the number of FTEs needed to respond to the data collection and reporting requirements.

I noted a few of the on-going quality projects in which HUMC is engaged; but in addition to these please be aware that our quality unit and our HIM departments receive an ever-increasing set of requests from third party payers and health plans, state agencies, researchers, and others seeking secondary data. It is the diversity of these requests, the lack of standards in process and data, and the fact that our industry has yet to achieve an interoperable electronic health record (EHR) that present many of the issues you appear to be addressing in your hearing today and the hearing in July.

HUMC, like most other healthcare providers and especially tertiary, teaching hospitals, had to consider the role of secondary data reporting as we established the processes and policies necessary to meet the requirements of the Health Insurance Portability and Accountability Act (HIPAA) law earlier in this decade. HUMC has established policies and procedures that reflect both the HIPAA and State of New Jersey confidentially and security requirements. Our on-going orientation and training reflect these policies and our understanding of the state and federal requirements.

I know over the last four years the NCVHS has followed the implementation and compliance with the HIPAA privacy and security rules and you understand that there still are situations where HIPAA requirements, when taken in relation to other federal and state requirements, create ambiguities when it comes to the release of secondary data. These uncertainties will increase as the community recognizes the value of secondary data especially as the healthcare industry migrates to a standard, interoperable EHR. If we are to have quality data and data integrity, the healthcare industry must address these ambiguities and improve the standards for secondary data reporting and collection across all spectrums of care.

**Authorization and Consent**

Ms. Amatayakul asked that I discuss patient authorizations, consent requirements, and policies related to quality measurement and other secondary data. As I have noted, HUMC, and I'm sure most providers, institutes simple policies, procedures, and "Notices of Privacy Practices" to comply with HIPAA and state laws. I have provided a few samples as attachments to my testimony. Typically, these policies and procedures have been adequate for the on-going secondary data reporting projects.

As you know, HIPAA does not require providers and health plans to obtain a separate consent for disclosures or access to protected health information (PHI) when it is disclosed or accessed for treatment, payment, or operations (TPO), and when required by law. HIPAA also provides exceptions for certain healthcare research disclosures and for disclosure of information that has been "de-identified." The remaining disclosures require an authorization for release or disclosure of information. All of these requirements are tempered by the state preemption section of HIPAA, so that if my state has a stricter requirement, the entity must follow the state requirement.

I have provided a table on Patient Authorization or Consent requirements for <u>secondary data</u> constructed to illustrate when consent or authorization is needed. This table assumes the individual has reviewed the HIPAA Privacy Notice and signed the initial releases for the entity that are normally required. You will note that there are a number of cells where, under HIPAA, the entity may not be required (subject to state law) to obtain an additional consent or authorization. There are a few situations where an authorization is required and there are several where we have put a question mark, because the release would be situational. The request for data, or the knowledge that a patient is

covered by a particular secondary data reporting requirement may not be known until after the individual is discharged. Many patients have multiple health plans or payers, and each may be associated with a variety of quality measurement programs.

Questions might arise in situations where the quality measurement or other data being sought does not potentially meet the TPO requirements. For example an entity might ask:

- If a quality measurement(s) is part of a requirement to receive payment; then can it be assumed that the release is covered by HIPAA-TPO? or
- Is the group requesting data a government entity, or a subcontractor of a government entity, as defined by HIPAA? Is the request covered by "as required by law" or TPO?

Question will also arise related to the requirement for "minimum necessary," for instance: What amount of the individual's record is minimum necessary, given the specific request and the entity requesting the information?

As noted, providers of secondary data are also faced with the dilemma that patients may be involved with one or more payers or health plans or multiple agencies desiring their healthcare information. While it might be perfectly appropriate to release data to a health plan that uses quality data for payment purposes, is it appropriate to provide such additional data to a secondary health plan that does not? How does minimum necessary apply to each? Just how do agencies and health plans use the data they receive under TPO – are they a covered entity or do other federal or state laws apply.

HIM professionals and others address these questions daily. Secondary data is produced from paper record, electronic records, and the majority today, from a hybrid of paper and electronic records. Most analysts will have to seek the requested data and answer these questions in this hybrid environment. In all cases, today, the analysis is a manual process. How will requests be handled in the future, when there is full adoption of a standard EHR and networked health information exchanges (HIEs), remains to be seen, especially if we anticipate computer assisted responses.

Fortunately, the number of requests beyond the TPO requirements today is relatively low, but as the healthcare industry moves towards entities that are fully "electronic" the demand for secondary data will and should increase to take advantage of all the interoperative data (knowledge) that is accumulated. The need to define who is requesting the data (raising authentication and authorization issues) will also rise, as well as the questions:

- What data are they requesting?
- Is it PHI?
- What right(s) does the individual have to restrict the data?
- How will the entity track or audit releases in the EHR system or through a HIE?

As the requests for secondary data increase, so will the need to train healthcare professionals and educate consumers on the various nuances associated with requests and requestors, as well as the laws, regulations, and rights in effect.

As consumers receive more information or misinformation about the use of healthcare data, data providers could find themselves more in a situation where consumer restrictions are placed on the release of data for external parties – except those "required by law." The users of secondary data along

with the entire healthcare industry must provide a clear picture as to how such data is used and the protections being provided to ensure such information is accurate, confidential and restricted to the purpose for which it was originally provided. Such education is needed for industry professionals as well as consumers. Feedback must be provided throughout the healthcare community to ensure that the data is used accurately and that if processes or collection of data needs to be changed the system actually will be changed.

I can assure the workgroup, audience members, and consumers that HIM professionals are making the effort to comply with existing laws and regulations and are working to see that laws, regulations, and processes are established to provide accurate data and ensure confidentiality. We hope that through a variety of efforts conducted by the NCVHS and others across federal, state, and the healthcare industry we can achieve a uniform understanding of what authorizations or consents must occur, when, and under what circumstances, so that we spend our time ensuring the completeness and integrity of our primary and secondary data, and not addressing the nuances of multiple and complex regulations.

**External Reporting of Secondary Data**

PHI data from the EHR

I noted that the requestor of secondary data not only impacts the decision of whether an authorization is required, but also the amount of PHI included in the data provided. Requests for secondary data, especially for quality measurement and public health must be judged not only for a TPO relationship, but also to determine any individual requirements for identification or de-identification. Some data is identified by name or a patient account number. Other situations call for a de-identification process where a separate identifier is used in case the patient needs to be informed of a situation calling for follow-up care. Such variation can be addressed in situations where only one payer, health plan, or agency is involved but the issue becomes more complicated when there are multiple plans or agencies similar to what I described above for authorizations.

Over time we expect to see additional information requested as secondary data. Metadata will potentially be required to determine the source of the data elements that make up a measure or a collection of data needed for reporting. Conversations are also developing around different initiatives to provide the individual with the ability to restrict specific information or data in their record. In addition to the potential requirement to sequester some data (which could in turn impact the integrity of secondary data), requirements for an accounting for data will potentially rises to ensure the disclosure limits are met. In a fully electronic system, such accounting and restrictions may not be a problem, but in today's environment they create significant administrative burdens. While an electronic environment will make some processes and protections easier, the ability to provide secondary data will continue to be difficult unless the healthcare industry and government can come to consensus on standards.

Standards for Data Reporting – Primary Data to Secondary Data

To meet individual consumer's expectations and the community's need for secondary data, HIM professionals and others have strived to create a primary record that can provide data that is complete and accurate. The development of uniform standards and other processes leading up to the adoption and use of standard EHRs are meant to ensure the standard EHR captures all the data necessary to

provide healthcare clinicians with information they need to care for and provide optimal treatment decisions for the patient.

First and foremost, the EHR serves as the primary health record for the patient. The record must be accurate and complete and insure integrity in data transfer among sub and external systems, data identification (metadata), and provision of data to ensure the clinical and business needs of the patient and the provider are met. While the record is for care, these same attributes are needed for the provision of secondary data. HIM professionals believe that given the demand for secondary data (some would have us believe this is the only purpose of the record) the community, the provider, and the patient are best served if the primary record's data can serve many purposes rather than the primary record itself becoming a hodgepodge of information collected specifically for a variety of secondary purposes.

Over time, as use of secondary data points to a need to modify the primary record, the healthcare community can determine what EHR and documentation standards need to be changed. Since there are many different requests for secondary data, this means that such requests themselves should be standardized and coordinated across the different sectors requesting data.

The role of the record analyst is to review the primary record and provide secondary data when requested or required. Many expect that eventually, with the adoption of a standard EHR, made up of uniform data (terminologies), some automation, via computer-assisted coding, will provide common forms of secondary data. If such simplification is to occur, some of the questions raised by the situations I previously noted must be resolved in a uniform manner, especially in the areas of quality measurement and claims-associated data.

To achieve administrative simplification through automation, we must ensure that our secondary reporting mechanisms, including contemporary classifications or codes can represent the primary record data, be accurately mapped to the primary record and to each other, and provide data to meet standardized secondary data requests. I must remind the workgroup of our quality workgroup discussion in 2004, when we discussed the failure of ICD-9-CM to convey adequate secondary information.

To protect the integrity of the primary record and automate some secondary data processes we must address the current conflicting requests for secondary data. The healthcare industry has not standardized either its quality measurements or the data that is accumulated to provide a quality measurement. The lack of standard measures, data definitions, and contemporary classifications also holds true for other categories of secondary data used for population health, health administration, and research. The lack of standardization makes the process of analyzing data for reporting difficult and can result in two different organizations (data requestors) having different results for the "same" measurement. This in turn can lead to confusion for consumers, as well as health professionals, a situation we have faced several times at HUMC.

Variance in data requests that often target the same output makes automating secondary data and ensuring data accuracy and integrity difficult. There is no standardization among organizations seeking quality monitoring let alone across the industry for research, population health, and administrative activities. While there are some national standards they are not necessarily followed on

a local or state level, and all standards and data definitions are typically complied with on a volunteer basis. AHIMA has been working on a request for information (RFI) from the Agency for Healthcare Research and Quality (AHRQ). It is my understanding that the RFI introduces the concept of an entity that could initiate and manage the coordination of secondary data measures, data definitions, and other attributes of secondary data requests so that data providers can report the data and maintain data methodologies that meet industry, government, and consumer expectations. This "data steward" model would deal with the process of developing data set standards, aggregation processes (including confidentiality and security), and coordination between standards and data users.

Needless to say, as a provider of data to a variety of outside organizations both state and national, anything that can be done to allow me to provide data in a uniform manner across the secondary data spectrum would be greatly appreciated. As a teaching and research facility sitting close to several other states I would appreciate not only the uniformity of secondary data requests and process, but also uniform confidentially and security requirements to follow for disclosure and transmission of data. I must also add that I also hope to see some means of requiring adherence to the standards and guidelines any "data steward" would produce. At this point, however, it does not appear that the proposed entity could mandate uniform use of standards and guidelines, a problem we have seen even with HIPAA standards.

AHIMA and the American Medical Informatics Association (AMIA) also recently released a white paper making similar recommendations with regard to coordinating terminologies and classifications, which serve as the basis for data in and reported out of the health record. This coordination will likewise be absolutely necessary if we are to have uniform reporting in an electronic health environment in the future.

Data Stewardship

Let me note that as a director of health information, I am a data steward. I have explained my role as it relates to consents and authorizations as well as in the release of secondary data to outside parties. Once this secondary data leaves my facility, by whatever means, some other entity takes on the responsibility as steward to the data that has been transferred. I have no control of their stewardship. They many have their own compliance requirements under HIPAA, IRB, or some other state or federal rule or law, but this may be doubtful, and certainly compliance varies. By some means, government and the industry must ensure that privacy protections extend to healthcare data, not matter where it exists or is stored. If individuals cannot trust the overall system, they will be reluctant to provide information in the primary record or they will add restrictions to the use and disclosure of data, diminishing the value of what secondary data can be produce and potentially endangering their health and the health of the population.

Internal Uses of Data

I also just want to note that HUMC also complies with HIPAA and state laws on the internal use of health information. The health information staff take great strides to de-identify data for the variety of research, teaching, and other functions that occur within the medical center, when needed. Our review of data to protect the patient occurs whenever data is used for purposes other than the actual diagnosis and treatment of the patient. Since so much goes on in a medical center, I cannot hope to describe all

the efforts taken on a regular basis, but I am ready to respond to your questions, if you have concerns in this area.

**Health Information Exchange**

The issues I have addressed so far have taken the perspective of a single data provider. I am aware that you are also considering the role of a HIE. Unless the HIE is itself a data repository, I do not see the HIE as the reporter of secondary data as I have just discussed it. Through a combination of policy and technology it may someday be possible that issues of identification, authorization, and consent might be addressed by an HIE. As the provider of the secondary data, a healthcare provider usually has a direct relationship with the individual consumer, I believe the decision points we have discussed are not currently at the HIE level. Without a clear model of an HIE it is difficult to say how an HIE made up of, or related to, multiple providers and other healthcare entities could or should address the issues of consents, authorizations and other confidentiality and security requirements.

AHIMA and AMIA have suggested that perhaps uniform legislation should be passed to prohibit the intentional misuse of an individuals' healthcare data or discrimination of individuals related to their healthcare data. Such a law could ideally permit the sharing of data for secondary purposes without a complicated set of rules pertaining to parts of the data base, identifiers, and so forth. Whether the healthcare industry or the governments in the US are prepared to take on such legislation and actually prosecute offenders is open to question as is how long it would take to pass such legislation into law.

**Conclusion**

This afternoon, I have only skimmed the surface of the issues facing HIM and this workgroup as we approach the topic of secondary data as it currently resides in a hybrid state of paper and electronic media or even just paper-based information, was well as a time in the future when all healthcare data will be electronic. I have tried to simply review the issues with consumer consent and authorization, along with a data providers approach to releasing secondary data with or without personal identifiers, review adherence to "minimum necessary" requirements, and acknowledge the lack of standards for process and data in the request and response to secondary data needs.

If the community as a whole is to benefit from the vast amount of healthcare knowledge that can be extracted for a fully interoperable healthcare system, then we must reach on-going, nationwide consensus on:

- Uniform use of authorizations and consents
- Uniform use of industry-wide terminology and classification standards in sync with international standards
- Uniform use of transaction and measurement standards to ensure consistent data collection across secondary data requestors for use by consumers and other entities working to improve healthcare and healthcare operation processes
- Uniform confidentiality policies and practices along with security measures to protect data that is both identified and de-identified, including issues related to authentication and accounting, if data requests become automated
- Education of consumers and the industry on the need for and use of secondary data and its relationship to primary data as well as how confidentiality can be guarded and increased in an

EHR/HIE environment. This also calls for strong legislation to punish discrimination and intentional misuse of health care data.

The healthcare industry must also address the mechanics of secondary data exchange including:

- The impact of the paper-hybrid-EHR transition, which will occur over the next decade. Reporting requirements must recognize this transition's affect on the data collected and the processes for collecting such data.
- The need for feedback in any secondary data system to ensure maximum use of the data and data accuracy as healthcare knowledge grows.

I have expanded beyond the issue of authorization and consents because my personal involvement with secondary data issues and the involvement of my profession raise the issues that need to be addressed. I suspect as this workgroup continues its hearings and deliberations additional issues will arise. For your additional consideration, I have also attached some practice briefs from the AHIMA that related to today's topic, recent statements on Quality Healthcare Data and Information and Confidentiality, and a summary of the AMIA/AHIMA recommendations on terminologies and classifications.

Whether today or in the future, if I or my professional association can be of any assistance to the workgroup or the NCVHS, please contact us. Again, thank you for allowing me the honor of testifying on this important subject. I stand ready to take your questions.

**Contact Information**

Barbara Siegel MS, RHIT
Director, Health Information
Hackensack University Medical center
Hackensack, NJ 06071

Telephone: (201) 966-2072
bsiegel@humed.com

Allison Viola, MBA, RHIA
Director, Federal Relatons
AHIMA
1730 M Street NW, Suite 502
Washington, DC 20036
Telephone: (202) 659-9440
allison.viola@ahima.org

i


**About the American Health Information Management Association (AHIMA)**

AHIMA is the premier national 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.

**Leadership in HIM Advocacy**

AHIMA has demonstrated leadership in legislative and regulatory issues at the federal, state, and local levels. Through a strong record of HIM advocacy in Congress; federal agencies; and standards development and maintenance organizations, AHIMA continues to improve the quality of medical records and advance opportunities for HIM professionals. Collaborative and advocacy efforts have focused on issues including the adoption of ICD-10, HIM workforce, privacy and confidentiality, consistency of coding, and the national health information infrastructure.

**Accelerating the Electronic Health Record**

One of AHIMA's areas of strategic focus is electronic health information management (e-HIM™). Its goals are to:

- Promote the migration from paper to an electronic health information infrastructure
- Reinvent how institutional and personal health information and records are managed
- Deliver measurable cost and quality results from improved information management

Acceleration of the electronic health record throughout healthcare is a collaborative process at the national level and within individual healthcare organizations. AHIMA works with industry leaders such as:

- American Medical Informatics Association (AMIA)
- Certification Commission for Healthcare Information Technology
- Connecting for Health project sponsored by the Markle Foundation
- e-health Initiative (eHI)
- Healthcare Administrative Simplification Coalition (HASC)
- National Alliance for Health Information Technology (the Alliance)
- State Level Health Information Exchange project

To enable its members to lead the transition to e-HIM™, AHIMA and Care Communications, Inc. have developed a two-day seminar based on principles of systems-based leadership and change management. The "Renaissance for the 21st Century: Leading the Change to e-HIM™ course is designed to help attendees develop personal action plans for change projects and personal and professional leadership development.

**Innovation and Advancement of Health Information Management**

Created in 1962, the Foundation of Research and Education (FORE) is a separately incorporated affiliate organization founded and managed by AHIMA. FORE provides financial and intellectual resources to sustain and recognize continuous innovation and advances in HIM for the betterment of the profession, healthcare, and the public.

- Workforce Assessment Study
- Merit Scholarships and Educational Loans
- Practice Solutions and Best Practice Awards
- Triumph Awards
- HIM Institute for Learning Excellence

- FORE Library
- Grant-in-Aid Research Awards
- Dissertation Assistance Awards
- Long Term Care Health Information and Documentation Guidelines

**Shaping and Improving Formal Education**
AHIMA serves as the accrediting agency for the nation's 286 college and university degree programs in HIM. Additionally, the association works with leading educators to advance curriculum models at all education levels and continuing education opportunities.

In 2004, AHIMA established an accreditation commission—the Commission on Accreditation for Health Informatics and Information Management Education (CAHIIM)—to serve as the sole and independent authority in all matters pertaining to accreditation of educational programs in health informatics and information management. CAHIIM grants accreditation status to degree-granting programs that have undergone a rigorous process of voluntary peer review and have met or exceed the minimum accreditation Standards as set by AHIMA in cooperation with CAHIIM.

**Setting Professional Standards of Excellence Through Certification**
As the certifying agency for the HIM profession, AHIMA issues credentials in health information management to ensure that its members meet professional standards of excellence. The Association awards the following credentials to HIM professionals possessing an associate's, bachelors, or postgraduate degrees in HIM and after completing a comprehensive examination:

- Registered Health Information Administrator (RHIA)
- Registered Health Information Technician (RHIT)

The following specialty certifications are also offered by AHIMA:

- Certified Coding Specialist (CCS)
- Certified Coding Specialist—Physician-based (CCS-P)
- Certified Coding Associate (CCA)
- Certified in Healthcare Privacy and Security (CHPS)

**Lifelong Learning and Professional Development**
To ensure that its members meet professional standards of excellence, AHIMA provides professional development opportunities and practice resources, including:

- *Communities of Practice*—a virtual meeting place for members to collaborate, network and reach out to peers with common interests, issues and areas of expertise.
- *FORE HIM Body of Knowledge*—part of *Communities of Practice*, this online library puts the entire breadth of HIM knowledge right at members' fingertips. It includes articles from the *Journal of AHIMA*, practice briefs, position statements, job descriptions, and more.
- *Journal of AHIMA*—a monthly journal delivering updated news covering HIM, practical guidance on new regulations and up-to-date policies and procedures.
- *Perspectives in Health Information Management*—an online scholarly peer-reviewed journal to promote the linkage of practice, education, and research and to provide contributions to the understanding or improvement of HIM processes and outcomes.
- *Advantage*—a member-focused newsletter assisting members in evaluating personal career strategies and understanding professional options.
- E-Learning—an online campus offering continuing education courses on HIM related topics 24 hours a day, seven days a week. E-learning offers no-travel convenience; instant feedback; and online study and testing options.
- Meetings—seminars and workshops where AHIMA members can actively exchange ideas and experiences across the country via satellite, telephone, and Web.
- Publications—books and electronic publications specifically tailored for the HIM field, all authored by working experts.

**For more information about the Association, go to www.ahima.org.**