Statement of

Mitchell Hansen, Vice President Enterprise
Systems and Services
Quest Diagnostics, Inc.

On behalf of

The American Clinical Laboratory Association

Before

U.S. Dept. of HHS AHIC
Confidentiality, Privacy & Security Workgroup
Hearing

September 29, 2006

Good afternoon. Paul Feldman, Kirk Nahra, Committee members and HHS staff, thank you for the opportunity to testify on behalf of the American Clinical Laboratory Association (ACLA), which represents national, regional and local laboratories. I am Mitchell Hansen, Vice President of Enterprise Systems and Services at Quest Diagnostics Incorporated. Quest Diagnostics is the nation's leading provider of diagnostic testing, information and services with more than 35 laboratories across the United States and in Mexico and the United Kingdom. We operate more than 2,000 patient service centers, where physicians send patients to have specimens collected, and employ more than 42,000 people company-wide. Each day Quest Diagnostics alone performs testing on more than 500,000 patients – over 140 million service encounters annually. The majority of these order and result transactions are facilitated via secure electronic exchange, such as our Care360 Physician portal, hub and bridge services to EMR vendors, and direct interfaces to customers' electronic health record systems or practice management systems.

We are, of course, just one laboratory company. As of June 2006, according to the CMS CLIA database, there are 120,534 laboratories, comprising 5,329 independent laboratories, 8,677 hospital based laboratories, and 106,528 physician office laboratories. As an industry, clinical laboratories are conscientious stewards of massive amounts of American's personal health information, and Quest Diagnostics and ACLA member companies appreciate the Committee's interest in hearing our perspectives about identity-proofing and user authentication as relates to requested disclosures of laboratory results.

Security and identity are paramount concerns for laboratories, given the substantial volumes of information that laboratories manage, exchange or support every day. It's worth describing some of the underlying processes that support identity management and authentication processes we use today.

The cornerstone for all of our HIT services is setting up a business arrangement, by which the primary caregiver and the laboratory exchange key information and which authorizes and sets forth both clinical and technical service expectations and levels of service. If a laboratory client is using a third party software system, terms also will be defined, assuming an agreement does not already exist. Once the business arrangement is set up, a unique account identity is then built in the laboratory clinical and supporting transaction systems, with validation controls at each exchange point within the laboratory information environment. With account (e.g., user) identity conclusively established within the laboratory domain, we implement the specified transaction exchange services, defining end-user security roles and identities, and configuration of authenticating hardware or communication keys as required. Frequently, additional testing ensues with the customer and/or systems vendor to insure nomenclature consistency, understanding and utility of special features, and an overall smooth process.

When the exchange is "live" in such a system, in other words, credentials and roles and responsibilities of persons receiving or accessing information have already been exhaustively and cleanly "proofed"; information sources, particularly patient identity, are therefore known quantities with little or no risk of confusion; physical devices involved in transaction exchange have been authenticated within the extended laboratory domain by known hardware, IP address, or VPN key; and finally, transaction timing and quality is assured for the consumer of the exchange by actionable service level agreements.

On the other hand, it is a significant technical challenge, and hugely costly, to progress from delivery of laboratory results to known business partners, systems, and appliances to try to support a broad extension of results query to an indefinite number of previously unknown caregivers, consumers, and unfamiliar electronic and personal health records systems. Before directly addressing the panel's questions, I would like to highlight several general topics that highlight some of our concerns.

First, on the basis of volume of requests alone, the inclusion of the end consumer (i.e., the patient) in the list of potential requestors will render identification and authentication virtually impossible to manage, particularly without any national patient identification number or tracking mechanism. A single individual presents in multiple unique roles -- for example, a single person acting as a direct consumer, a guardian consumer (e.g. a parent), a primary clinician, a secondary clinician (e.g. a specialist or other "copy to" recipient), or an institutional representative. For us, as a high volume national provider of laboratory services, we can estimate that an identity management solution would have to be required for hundreds of millions of individual, with many in multiple roles.

Queries by consumers will generate various issues even if a response to the query were technically able to be executed properly and delivered successfully – for example, lab results disclosed against the current wishes of an alienated spouse to his/her partner on the basis of an authorization made during happier times. As consumers become actively engaged in directing the flow of their health care information we can anticipate that they will choose to demand or limit this flow of information in ways we cannot now predict.

Today, established (i.e., authenticated) relationships only exist with a subset of clinicians

– those who order tests from the laboratory through an established business relationship. With regard to any extension of that system, a robust credentialing and authenticating facility – most likely manual - will be required to assure that, at a minimum, the following questions have been satisfactorily answered: (1) Is the requestor who they claim to be? (2) Does the requestor have the right to see this *general* type of information (e.g. a clinician would generally be granted access to medical data while a reporter would not)? (3) Does the requestor have the right to see the *specific* information requested? We are not aware today of any universally accepted operational definitions or rules that will support an automated or even semi-automated authentication authority in making this determination.

In regard to HIPAA, the mandated necessity to track, and disclose upon request, the inappropriate release of patient data is a relatively new regulatory requirement for covered entities. In the laboratory industry, most current disclosures of patient information occur within the context of client relationships. A future where clinical results data is broadly dispersed by ad-hoc query raises the spectre of accountability for inappropriate disclosure of PHI at multiple levels of ownership. Who will track and enforce restrictions on inappropriate disclosure at the consumer level, and what responsibility will be borne by the original providers of information? Further, if a patient wishes to restrict which clinicians see their information, how many times – and to how many different entities - does this need to be communicated? For example, a patient admitted to a hospital indicates that there are restrictions on how their medical information is to be shared, will need to have this wish transmitted to all secondary providers, such as the reference laboratory. By extension, then, all relevant patient authorizations and restrictions will need to be incorporated as required data elements on every single data transmission. But who will bear primary responsibility for maintaining and communicating these wishes to all in the health care provider supply chain? Since each laboratory accession is a new patient record, how will laboratories know the patient's intention with regard to disclosure of new laboratory records?

Finally, the Committee has indicated interest in understanding requests for "historical" data. This term is not defined and will likely pose a major issue for all health care systems, due to limited capacity to maintain all historical records in a query-ready state. Various laws and regulations do require specific record retention time frames for audits, legal inquiries, etc., but older data is typically archived and only produced upon request, within a reasonable time frame. With terabytes of data currently under management, we have a vivid understanding of the quantifiable cost of storage networks, as well as the overhead required to meet security, failover and disaster recovery requirements, as well as quality of service metrics for on-line response. There is no way to determine what the volume of potential "historical" requests will be if the consumer and provider expectation is that historical medical data will be query ready, regardless of time frame. What about multiple sources/copies of the data? For example, should the source of the data be the originating lab or the physician that ordered the test or the HIE that may in the future enable the exchange of such information? Do we all maintain copies?

To proceed to the first of your questions, automatic population from a laboratory data source to an EHR provides the most robust approach for assured identity management -- we would recommend that the authentication process between laboratory and EHR retain characteristics of today's process of establishing interfaces to a client system with all the assurances that process implies, regardless of technology. In this model, the electronic health record would be responsible for identify proofing the patient, and the EHR would establish, as a trusted agent, the necessary laboratory transaction exchange. Because most current laboratory information systems are focused on high volume, high quality clinical transaction management, creating system front-ends for consumer access, as well as supporting real-time collection or processing of inquiries, represent significant development cost and operational overhead to the laboratory industry.

The second question pertains to importation of information from Federal agencies and compliance with Federal information security practices. Although the Committee did not cite specific security practices, we feel that the expectation for Electronic Health Records to comply with information security practices is reasonable and that non-federal practices should not be different than federal practices where health information is concerned, as long as the requirements are reasonable and the cost of implementation is taken into consideration for reimbursement purposes. It's also worth mentioning that many federal data aggregation projects today mandate anonymized or psuedonymized data because the agencies don't have access rights to individually identified data. Clearly this precedent would be wholly incompatible with EHRs that are focused on creating individually-identifiable patient records.

Question 3: CLIA differentiates access to results based on state law. Electronic Health Records will likewise need to be compliant with all aspects of state and industry regulation and assume accountability for wrongful disclosure, as the laboratory industry does today in its clinical information transactions. This suggests strong identity proofing at all levels, to a standard appropriate to each individual and to the role, or roles, that they may play and the purpose for the request for disclosure of patient identifiable data. Our industry today would not release information to non-client physicians without strong identity checks to insure we are meeting compliance requirements and confirmation of a valid purpose for the disclosure that meets the requirements of applicable laws and regulations. Without clear and achievable security and authentication standards, and without standardized personal identity schemes and authentication clearing services, it will be as difficult, burdensome, and expensive for an EHR to authenticate identity as it would be for the laboratories today – essentially, a manual determination. Someone in the transaction will have to bear the costs, which will not be minimal.

Question four addresses the role of HHS in establishing identity proofing and user authentication. We would recommend that minimum standards be established along the lines of the HIPAA security rules – i.e., the types of systems and processes and procedures that must be in place for an EHR to perform identity proofing and user authentication. Consumers and providers will want to know which products conform to standards, suggesting that certification along the model of CCHIT could be valuable, and that ongoing certification audits could be required to assured continued adherence to the applicable standards. However, it cannot be the responsibility of each provider that supplies data to an EHR to verify that the EHR performs its functions in full compliance with federally established standards and in compliance with all applicable laws and regulations.

Regarding the pros and cons of automated vs. in person proofing, both the identity and purpose of the disclosure must be known, suggesting this might be best accomplished in a face-to-face meeting or other manual means, despite the fact that sheer volume and rising consumer expectations seems to favor an on-line process. In the case of consumers, it’s important to note that many patients (and certainly their guardians / representatives) often do not have specific information about all the health care organizations that have been involved in their care (e.g., names, dates, type of services) and would not even necessarily know where to find the information. Laboratories do not have direct contact with many – if not most – patients upon whom they perform testing making direct discussions with patients even more difficult. Referral testing performed by a reference laboratory on behalf of a hospital or by a specialty service under contract to a primary provider can further complicate this equation by distancing the testing facility from the patient who may not even know another laboratory was involved.

The most instructive related policies and procedures, as requested in item 6, probably exist in several of the on going interoperability projects, such as the ELINCS project administered by the California Health Care Foundation.

Regarding question seven, we would argue there is no “trade off” to be made balancing access and privacy concerns. The two are independent requirements. One cannot release health information to someone whose identity you have not conclusively established; in addition, that person MUST have a legitimate purpose for receiving the medical information – as provided under the HIPAA privacy rules. As stated in our introduction, the laboratory industry is steward to a significant amount of personal health information, and the potential for inappropriate disclosure at any level of the system will continue to be a concern for laboratories as access to test information evolves.

Finally, regarding concerns about the type and storage of information required for identity management, it is clear that by definition, interoperability requires the exchange of sensitive PHI. Our chief concern is that the cost of identity verification and authentication, plus the storage and management of this information is going to be quite high. It must be borne by someone. In addition to storage, access, and performance, a significant concern for all providers is managing the increased risk associated with proliferating PHI.

In conclusion, Quest Diagnostics and the ACLA appreciate the opportunity to present our views with you this afternoon regarding identify proofing and user authentication. We look forward to working with the Administration to meet the goals of the Community.