Testimony of Paul Jolly, PhD to the American Health Information Community Workgroup on Privacy, Confidentiality and Security September 29, 2006

I am Paul Jolly, a staff member of the Association of American Medical Colleges (AAMC), where I hold the title of Senior Associate Vice President. AAMC is a nonprofit association representing all 125 accredited U.S. and 17 accredited Canadian medical schools; nearly 400 major teaching hospitals and health systems, including 68 Department of Veterans Affairs medical centers; and 96 academic and scientific societies. Through these institutions and organizations, the AAMC represents 109,000 faculty members, 67,000 medical students, and 104,000 resident physicians. Additional information about the AAMC and U.S. medical schools and teaching hospitals is available at **www.aamc.org**.

I am pleased to testify for the Privacy, Security and Confidentiality Workgroup. My testimony will describe activities of AAMC, but the opinions I offer are my own and not necessarily those of my employer.

By identity proofing we understand the binding of an identity to an actual person. This is done at the hospital when a record is made of a birth, and it is done again by the Motor Vehicle Administration when a driver's license is issued. The MVA usually requires a copy of a birth certificate, which proves that a person with the claimed identity was born, but the MVA has no way of knowing that the person who presents the birth certificate is really the same person identified by the birth certificate. The person who is the applicant is bound to the identity with a photograph, accompanied by the issuance of an identification number. The MVA then issues a token – the driver's license – that may be used for authentication. From this time forward, a person in possession of this driver's

license and resembling the person in the photograph can successfully claim that identity.

The procedure for a passport is similar and in some ways not as strong, as the photograph is supplied by the applicant and not made by the agency at the time of registration.

The Association has considerable practical experience with identity proofing and user authentication, gained in operation of its computer based systems, in particular with the conversion of the Medical College Admissions Test (MCAT) to computer based testing. Our experience with this high stakes examination may provide lessons that will be applicable to health care professional and consumer access to electronic health records.

Identity proofing for the MCAT examination is based primarily on examination of a driver's license or passport, which takes place when the test taker appears at the test site. Our proctor of course compares the photograph on the identity document with the face of the person standing before him or her, but we also read the encoded information in the magnetic strip or bar code on the identity document and compare that with the printed identity elements on the face of the document. A driver's license with altered name or address would be exposed in this manner.

For future identity proofing, the MCAT has for many years collected a photograph supplied by the examinee and has obtained an inkless thumbprint on paper. As we make the transition from paper and pencil to a computer based examination, these procedures are being strengthened. We will now capture a digital photograph and digital fingerprints of both index fingers of the test taker when he or she first appears, then use

those biometrics to verify identity when the test taker returns from a break or appears for subsequent examinations. Most importantly, we intend to use the biometrics to verify identity of the students who appear for matriculation at medical school. We want to be sure that the person entering medical school is the same person who demonstrated adequate preparation on the MCAT. The new procedures are being phased in as the MCAT makes the transition to computer based testing and will be fully operational in 2007.

Strictly speaking, we can never be any more certain than we were at the initial identity proofing that a person owns the associated identity, but we can assure with a very high confidence that that association has been consistently maintained. If an examinee successfully assumes another's identity at the time of examination, he or she will have to continue using that identity through medical school and beyond. Because we enroll the identity with biometrics very early in a physician's career, it is less likely that a person would be motivated to assume another's identity in the first place.

An additional form of identity proofing that we have considered but have not implemented relies on the existence of a considerable quantity of publicly available data connected to identities. We might ask the applicant a series of questions that others would be unlikely to know. Sample questions might include, "In which of the following cities have you never lived." (followed by a list of four or five cities), or "If you come out of your front door and turn right when you reach the street in front of your house, what is the name of the first cross street you would encounter?" We have not used this method, in part because many of the young people who present themselves for the MCAT do not

yet have extensive public records that could be used for this purpose, but it might be useful for on-line registration of health care consumers.

For the MCAT, we employ user authentication when the examinee returns from a break, when a person returns for a subsequent examination, and as already mentioned when the student presents himself or herself for the first time at the medical school.

To accomplish the level of authentication described above, the Association will create a centralized database of identity and biometric data, to be accessed by medical school registrars and other authorized persons whenever a student needs to authenticate his or her identity. The fingerprints will not be submitted to the FBI and will not be used for background checks. We emphasize to the student that the use of the digital fingereprint protects them from identity theft whenever it can be used, as no one else can successfully masquerade as that student.

Persons who hear about this system for the first time, including students who wish to take the MCAT, may initially have some discomfort with the idea, associating it with privacy concerns. In the context in which we use it, however, we have encountered little resistance. The MCAT has been collecting thumbprints as a deterrent to fraud for decades, and the new system is seen as a more modern way to do the same thing. Students also recognize that this is a high stakes examination where fraud is a threat, and they accept the need for protective measures. It also helps to point out that our fingerprints and facial images are not really secrets – as we handle things and visit public places with security cameras, we leave them everywhere.

For access to laboratory data and other components of the electronic health record, there are potentially three types of users, the patient, the physician who ordered the test, and a physician who is involved in the patient's care but who did not order the test. For access to the data we need not only user authentication, but also authorization. The laboratory system will have both patient and ordering physician associated with the result in the laboratory information system, which will imply that both of these individuals are authorized to see the results. Authorization for a physician who did not order the test is separate, requiring patient consent, and a method will have to be found to include these consents in the information system.

For all three types of individuals, a user name and password or other authenticator will need to be assigned by system administration. The authenticator could be a simple password, but stronger methods are available and used in some places – Houston Medical Center, for example.

If the consumer has access to his or her laboratory results from the Internet, it makes no difference if access is desired from home or from a distant city. For physicians affiliated with the health system of which the laboratory is a part, the same is true. If it should be desired to grant access to physicians unaffiliated with the health system, however, new problems arise. The distant physician could register with the patient's health system, but in-person identity proofing would be impractical. A consulting physician with referrals from many different places would have to sign up with many different systems. The best solution for such cases would probably be some sort of federated identity management, where the new physician would authenticate himself or herself to his or her own health

information system and then access the desired laboratory with his or her identity verified by the physician's own system. Federated identity management systems are available and in limited use, but I have no personal experience with them.

The preceding comments have been general, but I can briefly comment on two of the specific questions posed by the workgroup.

In reply to question 3, it may well make sense to have more extensive procedures for identity proofing of physicians than for patients, because physicians will be ordering tests as well as reading results, and because they will have access to confidential information concerning their patients. More extensive identity proofing for physicians may be justified.

In-person identity proofing is definitely superior to a system that provides on-line registration, because the picture on the identification document can be compared with the appearance of the applicant for registration. Where an electronic fingerprint will be used for authentication, as it will be for the medical student at matriculation, observed collection of the fingerprint prevents spoofing with a plastic finger, a photograph of a fingerprint, and other frauds. On-line registration may be acceptable for consumers, where the registration entity has access to historical records involving the claimed identity, knowledge of which would be unlikely to be known by anyone other than the owner of the identity.

I believe AAMC's experiences with identity proofing and user authentication provide some lessons applicable to access by physicians and consumers to electronic health records. I would be pleased to answer any questions.