American College of Emergency Physicians®
ADVANCING EMERGENCY CARE

Hearing of the
National Committee on Vital and Health Statistics
Subcommittee on Privacy & Confidentiality
"Consumer Controls for Sensitive Health Records"

April 17, 2007

Hilton Embassy Row Hotel
2015 Massachusetts Avenue, NW
Washington, DC 20036

Testimony by

Brian F. Keaton, MD, FACEP
President
American College of Emergency Physicians (ACEP)

HEADQUARTERS
Post Office Box 619911
Dallas, Texas 75261-9911

1125 Executive Circle
Irving, Texas 75038-2522

972-550-0911
800-798-1822
972-580-2816 (FAX)
www.acep.org

On behalf of the American College of Emergency Physicians (ACEP), I'm pleased to have this opportunity to address the NCVHS Subcommittee on Privacy and Confidentiality regarding Consumer Controls for Sensitive Health Records.

ACEP is the largest specialty organization in emergency medicine, with nearly 24,000 members who are committed to improving the quality of emergency care through continuing education, research, and public education. ACEP has 53 chapters representing each state, as well as Puerto Rico and the District of Columbia, and a Government Services Chapter representing emergency physicians employed by military branches and other government agencies.

ACEP is committed to the development of the Nationwide Health Information Network (NHIN) linking all components of the healthcare system. To help make this happen, ACEP is dedicating significant resources to support standards development and the implementation of best practices. Emergency physicians like myself are playing vital roles in the development of regional health information organizations (RHIOs) which are the local and state building-blocks for the NHIN.

Emergency physicians are patient advocates dedicated to providing quality patient care and protecting the public's health, while also protecting the privacy and confidentiality of every patient's health information. While we respect patient's desires to control access to certain aspects of their medical records, we caution against the unintended consequences of a patient control policy that could impede our ability to deliver the best possible emergency medical care.

Emergency Department Care

Due to the very nature of emergency care, it is often delivered without the benefit of a patient's vital past medical information. Nevertheless, emergency care providers perform admirably as a safety net for this country's health care system, despite facing many complex issues, including increasing volumes, excessive patient waiting times, overcrowding, lack of surge capacity, ambulance diversions, specialty consultant shortages, and limitations in pediatric emergency care.

The Emergency Department (ED) serves many roles in our health care system. As the interface between the inpatient and the outpatient worlds, we manage the acute and often unexpected medical emergencies and traumatic events that result in hospital admission. In most settings, over 60% of hospital inpatients were admitted through the ED. We provide acute episodic care for patients who either have no access to their primary care, either because they're not in their home area or because they don't have that access, and we also provide care for those who are acutely ill or become acutely injured. We're experts at acute diagnosis and stabilization and we're also a vital link in the public health network. Moreover, the ED serves these roles on a huge scale: EDs serve the equivalent of 40% of the US population, annually.

The overriding reason for the creation of the NHIN and interoperable electronic health records is to improve the quality, efficiency, and safety of health care for all Americans. Providing patients control over sensitive, confidential information in the medical record has to be a high priority, but this must be balanced against the needs for timely data availability in an emergency care situation. As you know, ED care incorporates a vast knowledge base, and its clinical responsibilities are inherently time critical.

For implementation of an NHIN to be of maximal value in the emergency department setting, we must not surround it with measures and controls that could render it unusable by both patients and practicing clinicians like me.

Privacy and Confidentiality Safeguards

ACEP believes network operation should be consistent with current HIPAA rules and should include provisions to facilitate access for continuing care and emergency situations. We believe the Subcommittee’s consideration of patient control over sensitive health information in the medical record should be guided be the following principles, which we believe are critical to implementation of data systems that will allow us to provide the highest quality care to the millions of patients who seek care in our EDs every year.

1. **Optimal management of emergency cases requires <u>rapid</u> access to patient data.**

   Speed and reliability are crucial; if the system is not fast and always available, it will not meet the needs of clinicians and patients. A key finding of the May, 2004 Society for Academic Emergency Medicine Information Technology Consensus Conference was that, when caring for the emergency patient, *"Electronic clinical records should be released immediately upon the certification of a clinician that there is an immediate clinical need for the release of those records."* The issues of security, identification and authentication—as well as patient control—should facilitate that process rather than hinder it.

2. **The assumption must be made that a patient who is unable to give permission for data access would have done so had they been able to.**

   Our patients cannot always provide permission. Given the nature of emergency medicine, cumbersome or onerous authorization requirements must be avoided. Moreover, it is vitally important that a "break the glass" policy be included, whereby authorized emergency clinicians are able to quickly gain access to critical information with a doctrine of presumed consent when patients have emergency conditions and are unable to provide consent.

3. **Optimal management of emergency cases requires access to <u>complete</u> patient data.**

   Clinicians must be able to trust that the data they are viewing is complete and truthful. A single data point or set of data points obtained at a single point in time is like looking at a still photograph or a single frame of a movie. When we look at a movie, we're presented with sufficient frames per second to enable the brain to interpret the individual images as continuous action. Editing a movie to leave out or change significant portions can lead the viewer to reach incorrect conclusions. In a similar way, viewing incomplete data portrayed as complete can cause the clinician to reach unjustified and potentially dangerous conclusions. If know data is not accessible for any reason, the information system must call this gap to the clinicians attention in a very conspicuous manner.

4. **Emergency physician must be notified when a patient refuses permission to provide access to some or all of their data.**

   While ACEP does not disagree with a patient's right to withhold information, no matter how dangerous that might be, we believe it is critical that the treating physician be notified that the data being viewed is incomplete. Such refusal alters the "point of truth" and requires the emergency physician to look at the data differently.

5. **Public health needs, including syndromic surveillance, require reliable access to population-based data. Access to this data must be assured.**

   Secondary use of NHIN data should support improvements in public health through surveillance, benchmarking, and policy support initiatives. Critical de-identified public health data must be made available to maximize the effectiveness of surveillance systems, with or without the patient's permission. Also, once a risk is identified, there must be a link back from the de-identified data to the index cases for the protection of those index cases and the public.

6. **Some patients will refuse permission to access their data because they plan to injure themselves or others. We must provide provisions for allowing access to data critical to protecting the patient and society from the harm that could reasonably be expected to occur if critical data were not disclosed.**

   This is a difficult problem that may be beyond the scope of this committee, possibly requiring legislative action. Emergency patients are a subset of society as a whole. Some have ulterior motives for coming to the emergency department, including illegal and dangerous drug seeking behaviors, terrorist activity, etc. Others may represent a threat to themselves or others due to psychiatric conditions, intoxicants, or criminal activity.

7. **While not strictly under the purview of this committee, we would like to stress the fact that consideration must be given to the potential tort liability risks inherent to creation of a NHIN.**

   Two major legal impediments must be addressed if the NHIN is to be successful. The first involves liability for breaches of security, and the other involves liability for failure to notice or correctly interpret issues hidden in the vast volume of newly available results for tests that may have been ordered by another clinician.

Once again, thank you for providing this opportunity to address areas of concern to emergency physicians and the patients we serve.

***