Testimony of

Ralph W. Hale, M.D., F.A.C.O.G.
Executive Vice President
AMERICAN COLLEGE OF OBSTETRICIANS AND GYNECOLOGISTS

Cost and Confidentiality: The Unforeseen Challenges
of Electronic Health Records in Small Specialty Practices

Before the House Small Business Committee

July 31, 2008

Thank you, Madam Chairwoman, for inviting testimony from the American College of Obstetricians and Gynecologists (ACOG), representing our 53,000 physicians and partners in women's health, on confidentiality and cost concerns physicians in small practices face in the adoption of health information technology (HIT). The Committee has addressed this issue several times on behalf of small and solo practice physicians, including your March 2007 subcommittee hearing. We appreciate your commitment to understanding the implications of HIT for small specialty practices and for all of your work in the health care arena.

My name is Dr. Ralph Hale. I am an obstetrician-gynecologist, have served ACOG for many years in various volunteer capacities, and have been ACOG Executive Vice President, in charge of all its operations, since 1993.

America's health care system is at a crossroads in the development of HIT. In today's paper records system, a typical patient will receive screenings, tests, and procedures from multiple health care providers, often with little coordination or communication between these providers. Adoption of electronic medical records (EMRs) can help make sense of our increasingly fragmented health care system, improve patient safety, increase efficiency, and reduce paperwork.

We know we need to move to HIT, and HIT capability is maturing, but has it matured to the point where physicians, especially those in solo or small practices, feel confident in making such a large capital investment? Not yet.

HIT systems are not yet interoperable across small practices, insurers, and governmental agencies. Information privacy is too often treated as an afterthought. And HIT systems are very expensive, both in purchase dollars and in lost patient care hours.

These are some of the many issues that must be carefully addressed before we achieve a tipping point in adoption of electronic recordkeeping. Today I'll address two of the largest barriers to health IT adoption among ob-gyns and other physicians in solo and small practices: costs and confidentiality.

Costs

The system-wide benefits of HIT are many. Insurers will save by reducing unnecessary tests, patients will benefit from better care coordination and fewer medical errors. But these advantages don't necessarily translate into savings or revenue for physician practices.

Instead, physicians face Medicare and private insurance payment cuts. Little financial assistance is available for HIT investment. And uncertain interoperability standards and rapid technology changes can very quickly make this year's investment obsolete. Many physicians in solo and small practices are understandably reticent to take the HIT plunge.

The initial cost of purchasing HIT for a small practice is typically at least $50,000 per physician. Physicians face additional, ongoing costs in staff training and hardware and software updates as well. And it's important for the Committee to realize that while some assert that physicians can easily recoup HIT investments through greater efficiency and the ability to see more patients, many physicians see significant efficiency losses for months after upgrading to an EMR system.

In the last decade, insurance companies have pressured ob-gyns to compress office visits into a few short minutes. For many ob-gyns, the promise of EMRs is not to enable us to see more patients in the same day, but to take more time and provide better care to our patients. HIT can help us make those office visit minutes more meaningful, rather than shaving a few more minutes off of our time with our patients.

Bipartisan legislation approved last week by the Energy and Commerce Committee, H.R. 6357, the Protecting Records, Optimizing Treatment, and Easing Communication through Healthcare Technology Act of 2008 or the PRO(TECH)T Act, acknowledges the need for financial assistance with this investment, and we encourage Congress to increase support for start-up and ongoing costs associated with HIT.

Confidentiality

Confidentiality is critically important as medical information moves from paper charts to EMRs. Sensitive records of millions of Americans need to be protected and ethical dilemmas involving patient autonomy must be resolved. ACOG holds patient privacy and the confidentiality of a patient's medical records in the highest regard and respects the fundamental right of an individual patient to make her own choices about her health care. Protecting our patients' health information is of paramount importance.

Security Within the Physician Office

Within the physician's office, electronic recordkeeping can make a patient's record more secure. Even with the best office procedures, there is no way to know if an unauthorized person has taken a peek at a patient's paper file. HIT systems can block unauthorized viewers and keep track of when and by whom a record was viewed.

HIT systems should be compatible with HIPAA, and flexible enough to accommodate state privacy laws, a particular concern for ob-gyn care of adolescents. Every state has different laws regarding the age and to what care an adolescent may consent without a guardian's permission. Most state laws allow part of the record to be shared with only the adolescent and other parts with the parent. In addition, some services may require parental notification. HIT systems must integrate these complicated rules.

Balancing Patient Privacy and a Physician's Need to Know

The Value of a Complete Health Record

With interoperable, sharable electronic records, all physicians treating a particular patient can have the full story. A patient's paper record kept in her physician's office often shows only a slice of a patient's medical history, potentially missing important information from the patient's other physicians, including medication allergies, test results, and the results of particular therapies.

Without a shared electronic record, a physician relies on the recollection of each patient, which is often unintentionally incomplete. A patient may be uncertain about the name or dosage of a medication, not remember the date of a screening exam, or not have results of lab tests ordered by another physician.

Physician access to the full story with sharable EMRs is important to the care of all patients, and can be particularly relevant for patients with inconsistent contact with health care providers, including the uninsured and Medicaid beneficiaries. Often, these patients get their care in various settings, including physician offices, community clinics, and emergency departments. Since Medicaid and uninsured patients have greater instances of chronic diseases, they may greatly benefit from sharing medical information.

Respect for Patient Privacy

There are compelling reasons why physicians should have access to sharable, complete medical records. But there are also compelling reasons, based on respect for patients' privacy and rights to make their own health decisions, for limiting physician access to some patient medical information.

Some patients choose anonymous HIV testing or confidential testing for other sexually transmitted diseases (STDs) in order to keep test results out of their regular medical records. A woman may go to a family planning clinic for some care needs, but see her regular ob-gyn for other care. A woman may not want to tell anyone, including her regular physician, that she was treated in the emergency department for physical injuries from domestic abuse.

In many cases, the clinical benefit derived by a physicians' knowledge of very sensitive personal health information, like pregnancy termination in the distant past or an STD in college, may not be not significant enough to outweigh the patient's need for confidentiality and privacy.

And, even the best EMRs are not a substitute for talking with patients.

Finding the Middle Ground

To what degree should patients have control over the content of their EMRs? At one end of the continuum, patients would have no control over the content of or access to their records, and all the patient's physicians would have full access to all of the patient's medical information. At the other extreme, a patient may wish to block access to or delete important information from his or her medical record, leaving physicians with only some information.

ACOG has strong concerns about allowing patients to delete information from the record entirely. HIPAA allows patients to correct inaccurate information, but not to demand changes for other reasons. Allowing patients to alter a medically-accurate record would cause physicians to distrust all medical records.

Blocking access to selected information gives the patient significant control over her record, but may also limit a physician's ability to provide the best patient care. A treating physician is put in a very vulnerable situation as he's aware that some information is blocked from his view, but he has no knowledge of why, what that information is, or how it might affect his treatment decisions.

Patients are not always the best judges of what information is important. For instance, if a pregnant woman has a cat, her ob-gyn will want to inform her of the risk of toxoplasmosis, a potentially serious condition. Or a physician might want to know the weight of a patient's baby at birth, since birth weight of more than 9 pounds increases the patient's risk for diabetes. An ob-gyn can help a woman who has been the victim of domestic violence and becomes pregnant understand that pregnancy often triggers escalated partner violence and help her get the help she needs.

H.R. 6357, under the leadership of Chairman John Dingell, is a good start to guide us forward, while we develop financial and other incentives for physicians to purchase health IT and while we continue to find solutions to important privacy issues.

This massive undertaking requires physicians to trust their investment in health IT and patients to trust that their sensitive health information is protected. Success of a national health IT system depends on both.

We applaud your commitment and leadership on this issue, Mr. Chairman, and look forward to working closely with you and the Committee.

# # #