Testimony of

Mary R. Grealy
President
Healthcare Leadership Council

Hearing on

"HIPAA Medical Privacy and Transaction Rules: Overkill or Overdue?"

United States Senate Special Committee on Aging

September 23, 2003

Mr. Chairman, members of the Committee, thank you very much for this opportunity to testify on the issue of regulatory implementation of the Health Insurance Portability and Accountability Act (HIPAA). This is a matter of significant importance to America's patients, health care consumers and health care providers, and I appreciate being able to present the viewpoint of the Healthcare Leadership Council.

The Healthcare Leadership Council is a coalition of the chief executive officers of the nation's leading health care companies and institutions. The HLC membership embodies all sectors of health care – hospitals, health plans, pharmaceutical companies, medical device manufacturers, biotech firms, health product distributors, pharmacies and medical teaching colleges. Each and every one of our members is directly affected by the HIPAA privacy rule and, thus, HLC was and continues to be very involved in the development and implementation of the regulation.

The HLC also leads a coalition of over 100 organizations that strongly supports effective patient privacy protections. In fact, this coalition has supported legislation establishing national uniform privacy protections for health consumers. When the responsibility fell upon HHS, however, to put confidentiality protections in place, the coalition turned its efforts toward the development of a workable privacy regulation.

Before we discuss issues regarding the implementation of the HIPAA privacy rules – and there are significant issues that require attention – I want to spend a moment offering a broad review of the development and value of the regulation.

When it comes to this subject of patient privacy, every HLC member, every sector of the health care industry, has had the same concern and objective. How do we protect the sanctity of a patient's medical information privacy while, at the same time, ensuring that necessary information is available for providing quality

health care and conducting vital medical research? As well, how do you create effective confidentiality safeguards that do not burden providers and patients with unnecessary paperwork or delays in treatment?

We have the utmost respect for the officials in both the Clinton and Bush Administrations who wrestled with these issues and who diligently pursued a course that led us to the regulations we have today.

These regulations as revised by the current administration, while not perfect, do attempt to strike a balance between concerns about protecting personally identifiable medical information and the needed flow of information for treatment and research. Allow me to make four essential points about the value of these rules.

First, these regulations do exactly what they are intended to do. Disclosing identifiable health information for purposes other than carefully defined appropriate health care activities is prohibited unless the patient grants specific, prior written authorization. If you use a patient's medical record, without permission, for reasons other than legitimate health care purposes, you're going to be hit with federal civil and criminal penalties.

Second, patients are empowered by the modifications made by the Bush Administration in finalizing these rules. As now written, patients must be told how their information will be used and what rights they have to control their own data. This is an important step in giving patients greater control over their own personal information. We have always believed strongly, as well, that patients must have the right to review and amend their own records.

Third – and this is an important point when it comes to marketing – under the rules developed by HHS, patients will not receive marketing communications unless they actively opt in, unless they give their prior authorization. This is an

improvement over the original version of the rules, promulgated in the Clinton Administration, in which patients would have had to actively opt out of so-called marketing communications.

Fourth, and finally, these rules strike a vital and necessary balance when it comes to medical research. They maintain the "de-identification" of records in order to protect privacy, but give researchers access to information such as the patient's zip code or date of hospital admission. This information can be absolutely critical in tracing the outbreak of a disease. This is particularly important in light of our current bioterrorism threats.

Many potential difficulties in implementation were avoided when the regulations were revised last year. Under the Clinton regulations, patients would have had to give their written consent before they could receive treatment, receive a reminder to make an appointment, have your doctor schedule your surgery, or have a relative pick up a prescription for you. If these rules had not been revised, the more than three billion prescriptions filled last year and the hundreds of millions of hospital admissions and physician office visits would have been made more complex with unnecessary paperwork.

Even with these improvements, though, early implementation of the HIPAA regulations has clearly demonstrated that additional modifications are necessary. The rules' authors were wise to include a provision for the regulations to be revisited annually, to ensure that they are accomplishing their purpose without having unforeseen negative impacts on patients or providers.

As we look at possible modifications, we need to do so through the prism of quality patient care. Are any aspects of these regulations unnecessarily sapping resources, financial and human, from health care providers, resources that might otherwise be devoted to treating patients and pursuing improvements in health care quality?

Certainly, the price tag for implementing these regulations is a high one. The Department of Health and Human Services has estimated that the privacy rule will cost the private sector $17.5 billion over ten years. A study by Blue Cross Blue Shield – a member of HLC's confidentiality coalition – has placed the total costs even higher, stating that the total dollars spent on implementation, industry-wide, will be closer to $43 billion over five years. The important point here is that, regardless of whether implementation costs are $17.5 billion over ten, $43 billion over five or somewhere in-between, we're still seeing billions of dollars funneled toward regulatory compliance at a time when health providers are coping with fiscal austerity.

In fact, at a congressional briefing sponsored by HLC, just one health system – consisting of five hospitals and 1,400 beds – said their implementation costs had, thus far, totaled about $1.5 million. Extrapolate that total to the nation's health care system as a whole and it is easy to see that hospitals as well as all other health care providers are having to devote extremely large sums from their tight budgets in order to comply with HIPAA privacy rules.

In fact, wherever you look within the nation's health care system, you see entities having to carve dollars from limited revenues – dollars that could otherwise be devoted to patient care – to meet regulatory requirements.

- Marshfield Clinic, based in Wisconsin, analyzed the impact of just one small portion of the rule – the privacy notice requirement. The 660-physician group practice spent $75,000 – a cost that will continue to grow as new patients are added – to print, translate, sort and mail 200,000 privacy notices, as required by the rule.

- Concentra, a network of 244 occupational health care centers, spent $3 million on initial implementation of the privacy rule, including outlays

for consulting services, training costs, printing and other implementation activities.

- The National Association of Healthcare Access Management (NAHAM), a member of HLC's confidentiality coalition, is an association of organizations that provide oversight to patients and families as they enter the hospital system. NAHAM reports that the privacy rule is complicating existing processes that already meet the confidentiality needs of patients and that the regulations are adding a significant financial burden to an already taxed health care delivery system.

- Nursing homes, as well, are trying to find space within extremely tight budgets to comply with the HIPAA regulations. The American Health Care Association reported that it has spent nearly $1 million to provide educational materials on the rules to its nursing home members, and that is just a fraction of the compliance costs absorbed by the nursing home industry as a whole.

Clearly, it is necessary to undertake a comprehensive review of the regulations to determine how best to achieve the intent of the rules without forcing the expenditure of precious resources for non-essential compliance activities.

The American Hospital Association, also a member of the confidentiality coalition, has suggested, for example, that provisions regarding accounting for disclosures should be reviewed. Right now, the rule requires all covered entities to track the disclosure of patient health information (PHI) and maintain records on all patients – records that can be used to supply reports and disclosure statements on demand. At any time, an individual can request an accounting of PHI disclosures made by a covered entity for specific purposes. Individuals can request an accounting of all disclosures made over a six-year period.

What does this provision mean in practical terms? Let's look at the impact on just one hospital, Emerson Hospital in Concord, Massachusetts, a 145-bed community facility. Emerson will be required to document over 300,000 disclosures of protected health information each year. Let's assume that the tracking and recording of each disclosure takes one minute. That's 300,000 minutes, or 5,000 hours, per year – just to document disclosures in one community hospital. Again, extrapolate that to the nation's health system as a whole and you can understand the huge impact being felt by just one provision in these regulations.

At Emerson Hospital, compliance with this requirement means the hiring of two full-time employees whose sole jobs will consist of HIPAA-related paperwork. Assuming the average cost, in salary and benefits, for a clerical employee in Massachusetts, this will cost Emerson approximately $70,000 annually for regulatory compliance that provides only minimal patient benefits.

It is safe to say that only a very small percentage of patients will ask for a list of disclosure accountings after their care. Yet, under the privacy rule, Emerson must maintain a specific record of each disclosure in case a former patient should happen to request an accounting of all routine disclosures.

The American Hospital Association has provided to HHS a suggested change in this provision. Covered entities would develop a standard list of routine PHI disclosures that could be given to each patient who requests an accounting. This list would include, for example, the routine disclosures that are made for public health purposes – records of births and deaths, for instance. Covered entities would then only have to track non-routine disclosures for more detailed accounting reports. These non-routine disclosures would include those done, for example, for law enforcement reasons or to report suspected abuse.

As I said earlier in my testimony, constructing effective patient privacy regulations is, to say the least, a complex undertaking. Our most important challenge at this point is to make implementation of the rules as simple and meaningful as possible. Because of the regulations' complexity, we hope that the Office for Civil Rights responsible for its enforcement will take a real-world, common-sense approach. So far, we have every indication that they will.

This is particularly important in light of the fact that confusion still exists in various quarters on the rule's scope and implementation. Many companies in the medical device industry, for example, are not covered entities but have been asked by their hospital and physician customers to sign business associate agreements. Thus, they are affected by the HIPAA rule. Yet, there is considerable confusion and a lack of official guidance on the interaction between FDA regulations, international device standards, disclosures to foreign notified bodies for compliance purposes, and the HIPAA privacy rule.

It is essential that we never view these rules as a finished product, but rather as a meaningful regulation that must evolve and adapt with our constantly changing health care system.

We are doing our part at HLC, working with the confidentiality coalition, to assist entities with regulatory compliance. We have funded a million-dollar study that compares the new federal privacy regulations with existing state laws, so that providers and their business associates will know if they must comply with the state law, the federal rules or both. We are serious about compliance and helping hospitals, physicians, health plans and others with that effort. It should be noted, though, that as we illustrate this patchwork quilt of federal regulations and varying state laws, it further underscores the need for a single federal privacy standard affecting all patients and all health care entities uniformly.

Health plans and providers want to act as working partners with the public and with the government to ensure that people feel secure in their privacy, while at the same time making sure that we don't impede their treatment and research that will bring better health care in the future.

The good news is that this rule can be revised annually, so that the public will have the opportunity to seek necessary revisions. We look forward to working with this committee and with the Administration to ensure that federal patient privacy regulations serve the national interest as efficiently and effectively as possible. Thank you.