Congress of the United States
House of Representatives
COMMITTEE ON WAYS AND MEANS
1102 LONGWORTH HOUSE OFFICE BUILDING
(202) 225–3625
Washington, DC 20515–6348
http://waysandmeans.house.gov

April 26, 2002

The Honorable Tommy G. Thompson
Secretary of Health and Human Services
Hubert H. Humphrey Building
200 Independence Avenue, S.W.
Washington, D.C. 20201

Dear Secretary Thompson:

We write to commend the recent changes you proposed to the rule guarding the confidentiality of medical records (March 27, 2002, notice of proposed rulemaking published by the Department of Health and Human Services). These measured steps will improve patient care, encourage research, protect sensitive medical information and reduce administrative burdens imposed by the previous rule.

We are particularly pleased that you accepted our suggestions regarding the following changes:

- Elimination of the mandatory consent requirements;
- Simplification and clarification of waiver of authorization for Institutional Review Board review of research;
- Revision of the transition provisions for research use and disclosure;
- Clarification of the minimum necessary standard.

We continue to have additional concerns with the confidentiality rule, and encourage you to consider the changes outlined below.

Patient Consent Requirement

We fully support elimination of the mandatory patient consent requirement and strongly urge you to retain this change. This single change wiped away much of the underlying problems related to implementation of the rule. Patient care could have been seriously harmed if providers were required to obtain consent prior to treatment. However, we are concerned that the requirement that providers make a good faith effort to obtain written acknowledgement of a covered entity's notice of privacy practices will be confusing for patients and lacks any meaningful confidentiality protection. As such, we encourage you

not to implement this change, and simply require the notice to be provided without written acknowledgement.

Minimum Necessary

In addition, we support the clarification of the minimum necessary standard which adds a new provision to allow use or disclosure of protected health information "incident to a use or disclosure otherwise permitted" so long as the covered entity complies with other requirements of the rule.

Even with this change, we encourage you to eliminate the requirement because it is unworkable and would exacerbate medical errors. The requirement that a covered entity make reasonable efforts to limit the use or disclosure of identifiable information to "the minimum necessary to accomplish the intended purpose..." is unworkable because it injects subjectivity into decisions as to what information should be released, compromising the free flow of information essential to high quality care. Incomplete information will lead to a dramatic increase in inappropriate care.

Limiting the use of information in the course of treating patients within an entity such as a hospital, is an unnecessary and potentially dangerous proposition. It will harm patient care in two ways: by reducing quality and by increasing medical errors.

The IOM, in its report To Err is Human, concluded lack of information is a major cause of medical errors. Because providers determine what is necessary, and there are no penalties for under-reporting health information only for over-reporting, the incentive will be to release very limited information. It is difficult to understand how this will achieve consistency in use of information in the health care system as each information holder will need to determine the minimum necessary for use. This is directly counter to the Health Insurance Portability and Accountability Act's goal to simplify health transactions and reduce costs.

Finally, if the Department is unwilling to eliminate the requirement, we strongly encourage you to clarify or create an exception to the minimum necessary standard for data requested by covered entities to process standard transactions.

In addition, the confidentiality rule applies to oral communications in the definition of "health information." Because the HIPAA statute applies to information that is electronically stored or transmitted, inclusion of oral communications exceeds the rule's statutory scope, and therefore should be eliminated.

Definition of De-identified Data.

The confidentiality rule makes it more difficult and much more costly for researchers to perform broad-based studies that involve patient medical records rather than the patient themselves.

The regulation creates two processes for de-identifying medical information. The regulation requires nineteen different fields of information to be stripped from a patient's medical file in order to be considered de-identified. Alternatively, a statistician may use generally accepted statistical methods to certify that information is not identifiable if the risk of re-identification is "very small." Once a patient's medical record has been de-identified, information about the patient can be used freely, without the myriad restrictions imposed by the rule.

The requirement to delete the nineteen fields or that an individual can hypothetically be identified renders the medical records of little value. For example, researchers use zip codes and infant birth dates in epidemiological and clinical research, including biological and infectious disease tracking. Inclusion of birth date, date of admission, date of discharge, date of diagnosis, and/or other dates are necessary for investigators to conduct longitudinal studies that allow researchers to use historical medical data in developing new treatments. For example, patients treated for brain cancer with a combination of pharmaceutical and radiation therapy ten years ago, may provide new insights for researchers developing new biological products today.

The final rule requires not only the removal of important identifiers, but also requires that the entity not have knowledge that the data could be used alone or in combination with other information to identify an individual. Conceivably, any data set could be used or combined with other data to ultimately identify an individual. And while we would agree that any determined individual, including biomedical researchers, could conceivably link a patient's diagnosis with a zip code, for example, the goal of public policy relating to confidentiality protections should be to ***prohibit or punish*** inappropriate disclosure, not ***potential*** misuse. In this regard, the very structure of the rule points to its inherent weakness, and need for fundamental reform.

Business Associates

The NPRM proposes to extend to April 14, 2004 renegotiation of existing agreements and includes model business associate contract provisions. This provision exceeds the authority granted by the HIPAA statute and should be eliminated. HHS used this construct to extend the rule to all entities, even though HIPAA only applies to health clearinghouses, providers and insurers.

HHS proposed modification to delay implementation of the provision by one year is a recognition of the burdensome nature of the requirement.

Some hospitals have thousands of business associates and hundreds of contractors. The Joint Commission on Accreditation of Healthcare Organizations (JCAHO) noted to GAO that it would need to enter into contracts for each of the 18,000 facilities (including hospitals, nursing homes, home health agencies, and behavioral health providers) that it surveys for accreditation. Requiring new contracts and monitoring arrangements with each one would be costly and burdensome.

In addition, covered entities may be held liable for known violations of privacy requirements by "business associates" even though such actions are beyond the control of health care providers and despite the fact that the covered entity is in compliance with the regulation. The regulation also requires covered entities to have contracts with their business associate even if the business associate is a covered entity. Under the final rule, the first covered entity is liable for the acts of the business associate even though that entity has to comply with the regulation. The second covered entity should be held liable for violation of the rule.

At the very least the regulation should be amended to create a safe harbor for covered entities when a business associate violates the privacy rule. Parties that violate privacy, not their associates, should be held liable for their actions.

Again, we thank you for the major improvements you have proposed to the rule. It is far better for patients, researchers, and health care providers than the original rule. We hope you make these suggested additional improvements.

Best regards,

Bill Thomas
Chairman
Committee on Ways and Means

Nancy Johnson
Chairman
Committee on Ways and Means
Subcommittee on Health

WMT: jcw