

For Immediate Release May 25, 2006

Medical Privacy Amendment Defeated In HIT Markup

Americans' Privacy Left Unprotected As Medical Records Move From Paper To Electronic Files

Washington, DC The U.S. House Ways and Means Subcommittee on Health voted last night to deny Americans the assurance of medical privacy in the markup of the "Health Information Technology Promotion Act of 2005" (HR. 4157). The bill would "encourage the dissemination, security, confidentiality, and usefulness of health information technology".

In the Wednesday mark-up meeting Rep. Rahm Emanuel offered an amendment to add specific language to insure medical privacy and prohibit the improper use or disclosure of personally identifiable patient information. Key points were:

- Expressly recognize the individual's right to privacy with respect to the electronic disclosure of identifiable health information
- Require a patient's consent before releasing individually identifiable health information
- Allow patients to prohibit access to particularly sensitive information
- Provide for patient notification if their information has been lost, stolen, or used for unauthorized purpose
- Give patients the right to obtain damages for the improper use or disclosure of their information

The amendment was defeated by eight to five.

"Without these amendments, patients have no control over who sees and uses their medical records and are left vulnerable to companies that want to profit from patients' health histories or discriminate based on people's current and previous medical

conditions,” said Deborah C. Peel, MD, Chairman, Patient Privacy Rights Foundation.

Peel emphasized Patient Privacy Rights’ support for moving paper medical records to electronic files to improve health care and reduce costs, but not until stronger privacy and security protections are in place.

“If the Veterans Administration can’t prevent the data theft of 26.5 million names, Social Security numbers, and diagnosis codes for their veterans, why should patients believe their personal, sensitive health data is any safer in electronic files?” Peel asked.

In April, Peel’s Patient Privacy Rights and 25 other organizations, representing constituencies across the political and ideological spectrum, urged the U.S. House of Representatives to build a patient-centered system with patient privacy rights at the core of any national health information technology legislation.

On May 24, 2006, the Patient Privacy Coalition, including the Christian Coalition, the American Civil Liberties Union, the Family Research Council and Consumer Action, urged Congress to include a number of privacy protections in legislation, including preserving stronger state law privacy protections already in place. (See complete list of privacy recommendations below.)

Peel said HIPAA had become a “disclosure rule” and was “toothless” since the adoption by the U.S. Department of Health and Human Services of a 2002 amendment to the privacy law, which permits over 800,000 health-related businesses and government agencies to access personal health information without patient knowledge or permission. The 2002 regulatory changes allows health care providers to share patient records with employers, drug and insurance companies, credit reporting agencies, accountants, banks, lawyers, and others without patient permission, and for business and other uses unrelated to healthcare treatment or payment.

“The federal government’s own watchdog, the GAO, has repeatedly told Congress that HHS and the VA do not have adequate security protections in place for the health information

it handles for Medicare and Medicaid. Why should Americans trust an HIT network without the assurance of medical privacy,” said Peel.

The coalition recommended the following privacy protections:

- Recognize that patients own their health data
- Give patients control over who can access their personally identifiable health information across electronic health information networks
- Give patients the right to opt-in and opt-out of electronic systems
- Give patients the right to segment sensitive information
- Require audit trails of every disclosure of patient information and allow patients to review those disclosures
- Require that patients be notified of suspected or actual privacy breaches (The provisions in the Data Accountability and Trust Act should also apply to medical data.)
- Provide meaningful penalties and enforcement for privacy violations (Since February, 2005, over 52 million consumer records have been hacked.)
- Deny employers access to employees’ medical records
- Preserve stronger privacy protections in state laws (Ivo Nelson of IBM testified before an Energy and Commerce Health Subcommittee hearing in March that it would not be difficult to develop technology that follows individual state patient privacy laws in an interoperable national health data network.)