

For Immediate Release May 24, 2006

## **Medical Privacy Left Unprotected In Health Information Technology Bill Markup**

### **Bill Ignores Need for Patient Control of Medical Records**

Washington, DC - The privacy of Americans medical records has been left unprotected in today's U.S. House Ways and Means Health Subcommittee markup of legislation to build a national health information technology system, said a national consumer medical privacy watchdog group.

"Based on what we know about the bill, it gives patients no control over access to their medical records or right to keep their medical records out of electronic systems. That leaves all Americans 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.

"If the Veterans Administration can't prevent the theft of 26 million names and Social Security numbers from an electronic file, why would any patient believe their personal, sensitive health data is safe online?" said Peel. " Given the difficulty of preventing electronic theft, Americans should be able to opt-out of having online health records."

National research has shown that Americans will avoid treatment, be less than truthful about symptoms, omit critical medical data and delay care if they are compelled to share their medical records over electronic health networks without adequate privacy safeguards.

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 HIT legislation.

Groups, such as 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 (see below), including preserving stronger state law privacy protections already in place. Peel said none of these privacy protections have been included in HR 4157, introduced by House Ways and Means Health Subcommittee Chair Nancy Johnson of Connecticut.

“Congresswoman Johnson’s bill further undermines patient control by doing away with all state privacy laws that generally are much, much stronger than HIPAA, the federal Privacy Rule. Her own state, Connecticut, requires that patients give their consent before their medical records are released, while HIPAA has no such requirement,” said Peel.

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 600,000 health-related businesses and government agencies to access personal health information without patient knowledge or permission. The amendment allows health care providers to share patient records with employers, drug and insurance companies, hospital corporations, marketing firms, credit reporting agencies, accountants, banks, lawyers, and others without patient permission, and for business and other uses, unrelated to healthcare treatment or paying claims.

Peel emphasized Patient Privacy Rights’ support for moving from paper to electronic medical records to improve health care and reduce costs, but not unless ironclad privacy and security protections are put in place first.

“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 they handle for Medicare and Medicaid. Why should Americans trust another technology system that’s based on what’s not

working now?" said Peel.

The 19-member coalition recommends 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.)