



Healthcare

Services

FOR THE RECORD

DECLARE YOUR MEDICAL PRIVACY INTENTIONS

Health Care Services

The new federal medical privacy rule expands access to personal medical records and individually-identifiable patient data without patient consent, permitting and authorizing activities once considered unethical, unconstitutional, and impermissible.

In 1996, Congress passed the Health Insurance Portability and Accountability Act (HIPAA) which included a section called Administrative Simplification (AS) meant to rapidly advance the computerization and electronic transfer of health care information in the United States and around the world. The law requires creation of national codes and standards to enable electronic transactions of medical data, and mandates that **unique identification numbers be issued to all citizens**, health care practitioners, health care institutions, employers, and insurance companies—to facilitate linking and tracking of information. As recorded in *House Report No. 496, 104th Congress, 2nd Sess., at 99*, a member of Congress admits that facilitating access to medical data was the goal of AS:

"Health information is considered relatively 'safe' today, not because it is secure, but because it is difficult to access. These standards improve access and establish strict privacy protections."

PRIVACY IN NAME ONLY

Congress understood that requiring data to be computerized—and issuing a national medical ID number to all citizens—would generate great public concern over medical privacy. To address privacy concerns, they required the Department of Health and Human Services (HHS) to make medical privacy recommendations to Congress. But HHS's recommendations purported a new 'public responsibility' to share medical data for 'national priority activities.' When Congress failed to pass federal privacy legislation by August 21, 1999, HHS was required to write regulations to protect medical privacy. HHS received nearly 52,000 public comments on the proposed rule and over 11,000 comments and two citizen protest petitions on the final medical privacy rule. Despite citizen opposition to required and permitted disclosures of medical data, the final rule took effect April 14, 2001. Enforcement and implementation are set to begin April 14, 2003. The final medical "privacy" rule:

- *Requires* medical record disclosure to HHS inspectors at any hour on any day without patient consent or a search warrant, thus violating Fourth Amendment protections against warrantless government search and seizure of 'persons, houses, papers and effects.'
- Has a coercive consent provision that requires patient consent for sharing and using patient information for payment, treatment, and 'health care operations,' and allows providers and insurers to deny access to health care and insurance if the patient refuses to sign. The rule does however allow patients to *request*, but not necessarily receive, restrictions of uses and disclosures of data for hospital and facility patient directories, and restrictions of uses and disclosures of data to carry out payment, treatment and health care operations.
- Provides a broad definition of 'health care operations' that *includes but is not limited to*:

-medical necessity determinations	-quality assessments	-outcomes research
-clinical guideline development	-utilization review	-litigation/lawsuits
- *Permits* disclosure of individually-identifiable patient data, including social security numbers, without patient consent for many purposes:

-public policy and medical research	-law enforcement	-organ and tissue donation
-judicial and administrative proceedings	-"public health activities"	-health oversight activities

-government health databases

-serious threat to health or safety

-"emergency treatment situations"

- *Encourages* disclosures of medical information for 'critical national priorities' and the 'needs and rights of society as a whole.'
- Does *not* protect patient DNA, blood, organs, sperm, or other DNA-identifiable tissues and body fluids.
- Permits use of patient data for marketing by health care providers and health plans, and more limited use for fundraising purposes.
- Can only be enforced against entities covered by the rule: health plans, health care providers, health care facilities, and health care clearinghouses. The rule does not have authority over the use, re-use, or re-disclosure of data by law enforcement agencies, researchers, non-profit disease-specific organizations, foreign governments, business partners, organ donor organizations, most government agencies, and others who have data or are permitted to receive patient data from these 'covered entities.'
- Provides *no* individual right of legal action against persons or entities that violate the privacy and confidentiality of medical information.

Individuals should consider providing the following entities with CCHC's [Health Care Services Declaration form](#):

<i>Insurer/Health Plan</i>	<i>Pharmacy</i>	<i>Hospital</i>	<i>Physician</i>	<i>Healthcare Provider</i>	<i>Dentist</i>	<i>School</i>
<i>Government Agencies</i>	<i>Nursing Home</i>	<i>Attorney</i>	<i>Clinic</i>	<i>Data Clearinghouse</i>	<i>Employer</i>	<i>Psychologist</i>

Separate declaration forms addressing medical and personal data disclosures permitted by banks, creditors, life insurers, investment firms, and home health agencies by the 1999 Financial Modernization Act and the federal home health data collection system, called OASIS, can be found at the CCHC website: www.cchconline.org.

COPYRIGHT © CITIZENS' COUNCIL ON HEALTH CARE

"FOR THE RECORD" MEDICAL PRIVACY PROJECT, 2001

Citizens' Council on Health Care

1954 University Avenue West, Suite 8, St. Paul, MN 55104
Phone: 651.646.8935 / Fax: 651.646.0100 Email: info@cchconline.org