Robert Ellis Smith, Attorney,
Publisher of *Privacy Journal* newsletter
And *Compilation of State and Federal Privacy Laws*

State and Federal Laws Affecting Medical Confidentiality

17th HIPAA SUMMIT, September 16, 2009, Washington, D.C.

Health Information Tech Law of 2009 (Stimulus)

Amends HIPAA to (1) require breach notification, (2) permits patients to get an audit trail, (3) adds new entities to coverage of HIPAA, (4) limits mining and sale of patient data without consent, (5) disallows patient opt-out of electronic network unless self-paying, (6) permits use of patient data for fund-raising unless an opt-out, (7) authorizes state attorneys general to pursue HIPAA violations, (8) increases penalties of violations and requires training for HHS enforcement staff, (9) makes recipients of unauthorized disclosures criminally liable; (10) reiterates that providers must comply with stricter state laws, (11) creates an Office of National Coordinator for Health Information Technology with a policy committee to address privacy concerns.

Regulation under the HIPAA law of 1996

Provides patient right of access to own patient record and requires consent before many disclosures may be made; authorizes providers to use data to market their own services; extends confidentiality requirement to paper and electronic records.

States of Arizona, California, Colorado, Florida, Hawaii, Illinois, Massachusetts, Minnesota, New Hampshire, Rhode Island, Washington, and Wisconsin have laws protecting medical confidentiality. All but New Hampshire's predate HIPAA.

Also, there are partial protections in Georgia, Idaho, Nevada, and Tennessee.

Connecticut, Kansas, and New Mexico protect the confidentiality of mental health records.

Texas and Virginia protect patient records in state institutions.

Washington protects information in the state health-care financing system.

California in 2008: Providers must establish safeguards to protect patient data against "any unauthorized access, use or disclosure." A business may not obtain medical data from a patient for direct marketing with full disclosure of the uses and without consent.

New Hampshire in 2001: Patients must be assured confidentiality of all treatment. Patients shall be regarded as owner of the information. No release of patient data for marketing without written consent.

2008 Federal law on genetics limits access to and use of genetic information in employment and group health insurance. Does not preempt state laws. Does not limit a professional from requesting a genetic sample from a patient.

Laws in 34 states limit use of genetic information in employment decisions.

Laws in 41 states limit use of genetic information in insurance coverage.

A total of 18 states require HIV test results to be confidential.

Most states have law requiring patient access to own medical files.

State and federal laws relate to (1) hacking into a system or using a computer to commit a crime, (2) releasing medical information in credit reports and "insurance-support groups," (3) releasing information in school or university records, (4) releasing records related to drug or alcohol treatment, (5) disclosing individual data in insurance files (12 states), (6) community mental health and retardation centers, (7) certain third-party payor programs, like Medicare or Medicaid.

Medical information in federal agencies: The federal Privacy Act, which covers federal agencies and private entities that compile personal databases on behalf of the federal government, requires non-disclosure in most instances and provides a right of access and correction.

Patient records in Veterans Medical Centers are confidential by a separate law.

The Bottom Line

1. Has the patient knowingly consented to the disclosure? Consent is always a defense to a complaint of invasion of privacy.

2. Is the disclosure within the medical community to persons with a need to know?

3. Has the patient been given an opportunity to inspect and copy his or her own records?

4. Is there a viable plan for securing patient data?