State and Federal Laws Affecting Medical Confidentiality

Robert Ellis Smith

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?

Health Information Tech Law of 2009 (Stimulus)

Amends HIPAA

- **Requires breach notification**
- **Permits patients to get an audit trail**
- **Adds new entities to coverage of HIPAA**
- **Limits mining and sale of patient data without consent**
- **Disallows patient opt-out of electronic network unless self-paying**
- **Permits use of patient data for fund-raising unless an opt-out**
- **Authorizes state attorneys general to pursue HIPAA violations**
- **Increases penalties of violations and requires training for HHS enforcement staff**
- **Makes recipients of unauthorized disclosures criminally liable**
- **Reiterates that providers must comply with stricter state laws**
- **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.

Does not preempt existing state laws.

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

Medical information in federal agencies: The federal Privacy Act of 1974, 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.

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) confidentiality in community mental health and retardation centers, and (7) certain third-party payer programs, like Medicare or Medicaid.

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

A total of 41 states and D.C. require entities that experience security breaches to notify the persons who may be adversely affected, plus in some instances notify a state authority like the attorney general ("security-breach notification laws"). The laws in Georgia, Indiana, and Maine do not cover medical institutions.

Most states have laws requiring patient access to one's own medical files, HIPAA includes this.

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.

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.

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 without full disclosure of the uses and without consent.

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

Each of these laws is described, with the legal citation, in *Compilation of State and Federal Privacy Laws*, 2002, with a current 2009 Supplement, available in hard copy or electronically from *Privacy Journal*, orders@privacyjournal.net, www.privacyjournal.net

Beginning in the 1960s, the states of Arizona, California, Colorado, Florida, Hawaii, Illinois, Massachusetts, Minnesota, New Hampshire, Rhode Island, Washington, and Wisconsin have laws protecting medical confidentiality, and permitted patients to have access to their records. All predate HIPAA.

Florida's is typical: A licensed health-care provider must furnish copies of patient records to the patient or his or her legal representative, upon request, and may not disclose them to others without consent of the patient, except by subpoena.

Also, there are partial protections in Georgia (patient access, limits on disclosure of prescription records), Idaho (license may be revoked for betrayal of a professional secret), Nevada (the patient may forbid disclosure to third parties), and Tennessee (patient records in state facilities are protected; all patients may have access "upon good cause").

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

Tennessee, Texas and Virginia protect patient records in state institutions.

The ancient Hippocratic Oath requires confidentiality, but applies only to physicians, is not legally binding, and was generally not applicable to payment reimbursement.

The common law protecting privacy in the U.S. implies an obligation of medical confidentiality, starting with a landmark U.S. Supreme Court case in 1891 (*Union Pacific Railway v. Botsford*) holding that a woman could not be compelled to disrobe and submit to a surgical exam without her consent.

"No right is held more sacred, or is more carefully guarded, by the common law, than the right of every individual to the possession and control of his own person, free from all restraint or interference of others, unless by clear and unquestionable authority of law."

State and Federal Laws Affecting Medical Confidentiality

By Robert Ellis Smith, Attorney, Publisher of *Privacy Journal* newsletter

And *Compilation of State and Federal Privacy Laws*

Providence, Rhode Island

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