



## Medical Privacy

“One out of every six people engages in some form of privacy-protective behavior to shield themselves from the misuse of their health information, including withholding information, providing inaccurate information, doctor-hopping to avoid a consolidated medical record, paying out of pocket for care that is covered by insurance, and—in the worst cases—avoiding care altogether”—Georgetown University Health Privacy Project

The increasing intrusiveness of data gathering conjures up a future when consumers risk losing control over how their sensitive personal information is used. In reality, that future is now.

Electronic storage of information has changed our lives in many positive ways and has many beneficial uses in the health care arena. For example, ready access to complete electronic medical records can reduce medical errors caused by missing a critical fact such as a drug allergy. Electronic prescriptions are far clearer than physicians’ often illegible prescriptions.

But electronic medical information also presents dilemmas – the most prominent being the protection of sensitive and highly personal health information. Americans consistently support strong protections for the privacy of individually identified health information.

Consumers Union supports federal privacy policies that establish a basic level of protection nationwide. We also support strong state policies, with state regulators keeping a close watch to ensure that Texans’ personal health information will be kept confidential. Health privacy policies should cover the following:

**RESEARCH AND HEALTH DATABASES.** “With proper safeguards against re-identification, analysis of government, hospital, and health care databases yields a gold mine of information on public health trends and the effectiveness of various types of care,” Consumer Reports states. Safeguards include assigning unique patient identifiers with strong penalties for anyone attempting to re-identify a patient; a science review panel which screens and allows only legitimate researchers who agree to use the data for specific purposes; suppression of small elements of data and coding of data that might allow identification. The Texas Health Care Information Council uses all of these safeguards, and more, to ensure patient confidentiality is not breached.

- **Notice** Clearly inform consumers of health care services, in understandable language, about how their health information is collected, how it will be used and to whom it might be disclosed.
- **Consent** Allow consumers to limit the use of personal health information *beyond the purposes for which it was originally intended*. An “opt in” approach, under which consumers must explicitly grant advance permission to share information for other purposes, should be the standard.
- **Access** Give consumers the

right to a timely and inexpensive way to view, copy and correct inaccuracies in their own health records.

- **Security** Require health care providers, insurers, and other health entities that gather or use information about consumers to comply with privacy laws and to reasonably ensure the information is secure against loss or unauthorized access or use.

- **Enforcement** Impose strong penalties for privacy violators, both civil and criminal. Self regulation is not enough. Regulators must be funded to investigate violations. Consumers should have the right to a private cause of action when they have been harmed by the release of health information.

### In Short

Although new federal “HIPAA” rules help protect individual medical information, the state can and should do more. Drug companies, for example, collect substantial health information and are exempt from HIPAA requirements. Further state enforcement will ensure compliance.

**WHAT IS HIPAA?** HIPAA, the 1996 Health Insurance Portability and Accountability Act, required the federal health agency to adopt regulations if Congress failed to pass comprehensive health privacy legislation. These regulations were finalized in December 2000. Consumers support the HIPAA regulations because they give patients access to their records; limit others’ access to protected health information without specific consent; and restrict employer access to their employees’ protected health information.

While these federal regulations provide a baseline, they don’t go far enough. They don’t cover drug companies or life insurers and fail to give consumers a cause of action if they are harmed by released information. States need to pass more comprehensive protections with state enforcement. A privacy ombudsman should inform the public about privacy rights.