



Health Record Banking Alliance

12/24/10

State Legislative Principles **Recommended by the Health Record Banking Alliance**

These principles are designed to serve as guidelines for state legislation to promote health record banks and protect consumers who use them. Specific legislative provisions will depend on a particular state's laws. These recommendations are offered in the absence of existing comprehensive federal legislation specifically preempting the field.

I. Definition

A health record bank or trust (HRB) is any organization that provides an electronic repository for storing and maintaining an individual's comprehensive health and medical records from multiple sources (including the individual).

II. Overview

- A. HRB records should not be classified as medical records subject to the existing state laws governing such records because they are privately owned and controlled by the consumer.
- B. HRB records should be considered the property of the consumer, and therefore civil and criminal penalties should apply to anyone misappropriating, altering, or granting access to them without the explicit digital or other written consent of the consumer.

III. Ownership of Information

- A. All information in an HRB account is the property of the consumer.
- B. All access requires consumer permission.
 - 1. All access is recorded in audit trail (saved for a limited time period).
 - 2. Consumers have access to their account audit trail.
- C. An HRB shall have no liability as a consequence of honoring requests of consumers to release or withhold any portions of their information.
- D. Willful disclosure without consent is a felony.
- E. Negligent disclosure without consent is a misdemeanor.
- F. Federal breach notification rules apply.
- G. An HRB is authorized to receive laboratory results for all persons who have accounts, and all HRB account holders are authorized to receive their own laboratory results [*i.e.*, states should opt out of the federal Clinical Laboratory Improvement Amendments of 1988 - CFR Title 42 § 493].

IV. Consumer Protection

- A. The sender of all information must be indicated with the information.
- B. Consumers must have 24/7 electronic access to their data.
- C. A Health Record Bank must establish authentication procedures for all users, preferably using at least two factors (consistent with The National Strategy for Trusted Identities in Cyberspace, see <http://www.whitehouse.gov/blog/2010/06/25/national-strategy-trusted-identities-cyberspace>).
- D. Consumers may allow others to access some/all of their data with electronic 24/7 access.
- E. Consumers may delegate another person to manage their information.
- F. Use of information for research, public health, and public policy is by consent of each user whose information is incorporated into any disclosure (Exception: HRBs are required to report all information subject to other legal and regulatory requirements, *e.g.*, public health, law enforcement, national security).
- G. Health Record Banks must establish processes for correcting errors by updating, amending, and sequestering data, including mechanisms for notification of parties who have received such data.
- H. Consumers are entitled to an electronic copy of their data upon closing their account, after which all data on file will be destroyed within 60 days. HRB must retain information until the consumer closes their account or at least one year after the death of the consumer (unless the consumer instructs otherwise, *e.g.*, through advance directive).
- I. All holders of medical record information are required to send copies of the information in a reasonably available standardized digital format (other than facsimile) as soon as reasonably practical after requested by the consumer or the information is created, but in no case more than 24 hours after such request or creation, to an HRB account designated by the consumer. A consumer request for such transfers must be honored until cancelled by the consumer.
- J. Existing state consumer protection laws shall apply to HRBs.

V. Liability

- A. An HRB shall have no liability for incorrect information it receives.
- B. An HRB shall have no liability for improper data releases caused by a user's failure to protect their identity and authentication credentials.
- C. An HRB shall have a limit of liability to an individual of \$10,000 for a single data breach absent any willful and malicious conduct by the HRB.

VI. Regulation

HRBA supports government oversight of HRBs as the industry evolves, but believes that federal regulation via pre-emption is preferable and would be more efficient because many HRBs are likely to operate in multiple states.