



California Healthcare Medical Billing Identity Theft Prevention Program

California Healthcare Medical Billing Name ("CHMB") has developed this Identity Theft Prevention Program pursuant to the Federal Trade Commission's Red Flags Rule , which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. 16 C. F. R. § 681.2. In addition to possessing “covered accounts”, under the Red Flag Rules, CHMB also meets the definition of *Service Provider* to its customers that are medical practices. In this regard, CHMB will perform its activities defined in the customer services agreement in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft, as required of a *Service Provider* under the *Rules*. CHMB is committed to protecting the identity of its customers, as well as the medical identity of its customer’s patients. Medical identity theft is a serious problem. It can lead to inappropriate medical care when incorrect information is included in the patient's medical record, as well as cause financial problems for the patient. This Identity Theft Prevention Program sets forth the steps and implements internal controls to identify, detect, prevent and mitigate the identity theft of both customers, and customer’s patients. After consideration of the size and complexity of CHMB’s operations and account systems, and the nature and scope of CHMB’s activities, the Board of Directors_determined that this Program was appropriate for CHMB, and therefore approved this Program on November 1st, 2008 and updated on June 29th, 2009.

CHMB identifies 14 red flags in considering the types of accounts that it offers and maintains, the methods it provides to open and access its accounts, and its previous experiences with Identity Theft. Listed below are the preventive/protective measures upon their detection.

Prevent and Mitigate

1. Continue to monitor an account for evidence of Identity Theft;
2. Contact the customer;
3. Contact the Practice administrator
4. Change any passwords or other security devices that permit access to accounts;
5. Not open a new account;
6. Notify the Program Administrator for determination of the appropriate step(s) to take;
7. Notify law enforcement; or
8. Determine that no response is warranted under the particular circumstances.

Protect Customer Identifying Information

In order to further prevent the likelihood of identity theft occurring with CHMB accounts, CHMB will take the following steps with respect to its internal operating procedures to protect customer identifying information:

1. Ensure that its website is secure or provide clear notice that the website is not secure;
2. Ensure complete and secure destruction of paper documents and computer files containing customer information;
3. Ensure that office computers are password protected and that computer screens lock after a set period of time;
4. Keep offices clear of papers containing customer information;
5. Request only the last 4 digits of social security numbers (if any);
6. Ensure computer virus protection is up to date; and
7. Require and keep only the kinds of customer information that are necessary for billing purposes.

Additional measures in regards to communication are as follows:

- Take reasonable steps to verify his or her identity. Prior to releasing any information, staff must ask the caller to verify the following two sources of information:
 - *Last four digits Social Security number or mailing address*
 - and*
 - *Date of birth*

This Program will be periodically reviewed and updated to reflect changes in risks to customers from Identity Theft. At least once per year, the Program Administrator will consider CHMB's experiences with Identity Theft situation, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, changes in types of accounts CHMB and its customers maintain and changes in CHMB's business arrangements with other entities. After considering these factors, the Program Administrator will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Program Administrator will update the Program or present the Board of Directors with his or her recommended changes and the Board of Directors will make a determination of whether to accept, modify or reject those changes to the Program.