

ANESTHESIA BILLING, INC.	IDENTITY THEFT PROGRAM
Effective Date: October 1, 2009	

1. PURPOSE

To establish a written Identity Theft Program (“Program”) for Anesthesia Billing, Inc. ("ABI") designed to detect, prevent, and mitigate identity theft consistent with the Federal Trade Commission’s (“FTC”) regulations surrounding Identity Theft (also known as the "Red Flags Rules") as set forth at 16 CFR Part 681.

2. DEFINITIONS

2.1 Covered Account. A Covered Account means: (1) any account ABI offers or maintains primarily for healthcare provider payment purposes that involves multiple payments or transactions, including one or more deferred payments; and (2) any other account ABI identifies as having a reasonably foreseeable risk to patients or to the safety and soundness of ABI from Identity Theft. For purposes of the Program, Covered Accounts shall include any accounts providing for the deferred payment of charges by patients (including deductibles and co-payments) after health care services have been provided.

2.2 Identifying Information. "Identifying information" is any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including but not limited to: any name, social security number, date of birth, official State or government issued driver’s license or identification number, government passport number, employer or taxpayer identification number.

2.3 Identity Theft. Identity Theft is fraud which is attempted or committed by using the identifying information of another person without authority.

2.4 Red Flag. A Red Flag means a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.

3. PROCEDURES

3.1 Identification of Red Flags. Exhibit A describes the Red Flags that have been identified as most relevant to ABI. The Red Flags generally fall within one of the following general types:

1. Suspicious documents;
2. Suspicious Personal Identifying Information;
3. Suspicious or unusual use of a Covered Account;
4. Alerts from others (*e.g., patient, Identity Theft victim, or law enforcement*).

3.2 Detecting Red Flags. ABI typically has no pre-existing relationship with the patients and ABI has no reasonable opportunity to obtain patient demographic or billing information directly from the patient (or to verify the patient's identity). This information is provided to ABI by the clients (health care providers) which have adopted their own policies and procedures for the detection of Red Flags and possible identity theft. Accordingly, ABI will rely upon the clients' registration and Red Flag procedures as the primary means of detecting, preventing and mitigating the effects of identity theft. If a client notifies ABI of a Red Flag or identity theft issue relating to one of the client's patients, ABI will follow the procedures described in Section 3.3 of this policy as applicable to the situation.

3.3 Preventing and Mitigating Identity Theft. In order to prevent and mitigate the effects of identity theft, ABI staff will follow the appropriate steps identified in the attached Protocol for Investigating and Responding to Suspected or Confirmed Identity Theft (Exhibit B). As provided in that Protocol, appropriate responses to suspected or confirmed Identity Theft may include:

- Monitoring a covered account for evidence of identity theft;
- Notifying the client whose services are being billed;
- Contacting the patient directly;
- Changing any passwords, security codes, or other security devices that permit access to a covered account;
- Reopening a covered account with a new account number;
- Not opening a new covered account;
- Closing an existing covered account;
- Ceasing attempts to collect on a covered account;
- Notifying debt collectors;
- Notifying third party payors;
- Notifying consumer reporting agency, if adverse report made;
- Notifying law enforcement;
- Determining no response is warranted under a particular set of circumstances.

3.4 HIPAA Compliance. In the course of investigating, responding to, and mitigating the effects of Identity Theft, ABI and its staff shall comply with applicable laws regarding the confidentiality of health information including but not limited to the privacy provisions of the Health Insurance Portability and Accountability Act and 45 C.F.R. Parts 160 and 164 (collectively "HIPAA"). Without limiting the foregoing, ABI shall not disclose any protected health information of a victim or a perpetrator of Identity Theft to any party including law enforcement unless ABI's President has determined that such disclosure is permitted by applicable law.

3.5 Program Administration. ABI's President ("Program Manager") is responsible for developing, implementing, administering, and updating the Program in accordance with the procedures established herein.

3.6 Annual Review. At least annually, the Program Manager shall determine whether updates to the purpose and scope of the Program are appropriate. When making this determination, the Program Manager shall consider changes in the risks to patients and ABI from identity theft and changes in the business arrangements of ABI.

3.7 Subcontractor Arrangements. ABI will require, by contract, that all subcontractors that perform activities in connection with Covered Accounts have policies and procedures in place designed to detect, prevent, and mitigate the risk of Identity Theft with regard to Covered Accounts. The Program Manager will develop procedures to implement this Program requirement.

3.8 Updating the Program. The Program Manager will periodically review the effectiveness of the Program and update the Program to reflect changes in Identity Theft risks, methods of preventing Identify Theft, and other circumstances.

3.9 Training. The Program Manager will be responsible for developing a training program for staff identified by the Program Manager as having a role in implementing the Program. Staff shall be notified of Program updates through such education and training.

4. REFERENCES

Federal Register, Vol. 72, No. 217, November 9, 2007, p. 63718-63775
16 CFR Part 681

Exhibit A

List of Identity Theft Red Flags

This document provides a list of Red Flags that may indicate the possible existence of Identity Theft. This list is not all-inclusive; other facts and circumstances may suggest the possibility of Identity Theft. When a Red Flag or any other indicator of possible identity theft is detected, ABI's staff shall follow the procedures described in the Protocol for Investigating and Responding to Suspected or Confirmed Identity Theft which is provided as Exhibit B.

Suspicious Documents.

- Documents with information inconsistent with existing customer information (e.g., a person's signature on a check appears forged);
- Forms that appear to have been altered or forged; and
- Other suspicious use of a document reasonably identified through previous experience;

Suspicious Personal Identifying Information.

- Identifying information presented is inconsistent with other sources of information (e.g., an address not matching an address on a credit report);
- Identifying information presented is the same as information shown on other applications that were found to be fraudulent;
- Identifying information presented is consistent with fraudulent activity (e.g., fictitious billing address);
- SSN is the same as one given by another patient;
- Discrepancies in address or phone number;
- A person's identifying information is inconsistent with information on file for the patient (e.g., gender or ethnicity mismatch); and
- Other unusual use of personal identifying information reasonably identified through previous experience.

Suspicious Account Activity.

- Attempts to access an account by unauthorized users;
- Breach in ABI's computer system security;
- Other unusual use of or other suspicious activity related to a Covered Account reasonably identified through previous experience;

Alerts from Others.

- Notice from victims of identity theft;
- Notice from law enforcement authorities; or
- Notice from other persons regarding possible identity theft in connection with Covered Accounts.

Exhibit B
PROTOCOL FOR INVESTIGATING AND RESPONDING TO
SUSPECTED OR CONFIRMED IDENTITY THEFT

1. Staff Responsibilities. When a Red Flag is detected, ABI's staff shall make initial inquiries for the purpose of assessing whether there is a legitimate explanation for the Red Flag or whether Identity Theft may be a concern. The staff shall notify the Program Manager or his/her designee of the Red Flag and the results of any inquiry. If the Red Flag was not resolved by the initial inquiry, the staff shall defer opening any new Covered Account pending authorization from the Program Manager or his/her designee.
2. Program Manager Responsibility for Follow-Up and Mitigation. After receiving notification of a Red Flag or other circumstances indicating the possible existence of Identity Theft, the Program Manager, or his/her designee, shall complete the investigation of the suspected activity, report the activity, and/or take other appropriate action to respond to and mitigate the effects of the suspected or confirmed Identity Theft. Such actions may include, without limitation, monitoring a Covered Account for evidence of Identity Theft; changing passwords, security codes or other security devices that permit access to a Covered Account; declining to open a Covered Account; reopening a Covered Account with a new account number; closing an existing Covered Account; notifying the client whose services are being billed; ceasing collection efforts on Covered Accounts or instructing collection agencies to cease collection efforts; if payment received from third party payor, notifying payor of Identity Theft or if an adverse report had been made to a consumer reporting agency, notifying the agency that the account was not the responsibility of the victim. The Program Manager, or his/her designee, shall determine what reporting and follow-up actions are appropriate and shall document all actions taken in response to the suspected Identity Theft. The Program Manager may delegate the responsibility for some or all of these steps as provided in Program Protocols.
3. Notice to Law Enforcement. If, after completing an initial investigation, Identity Theft is suspected, a report should be made to the local police department. Typically, a case number will be assigned if the officer takes the report over the phone. The name and badge number of the officer taking the report and the case number should be recorded by the reporting party. The reporting party should coordinate with the police department regarding the timing and content of

notice to the suspected victim as described below. The information reported to the police should be limited with all protected health information deleted: Do not provide any medical information (including history, diagnosis, reason for visit or services rendered) of the suspected victim or person treated. Total charges are acceptable.

4. Reports to the Federal Trade Commission. Incidents of Identity Theft should be reported to the Federal Trade Commission (“FTC”) at 877-438-4338 or <http://www.consumer.gov/idtheft/>. A reference number will be provided for ABI’s records. This number and the operator number of the FTC representative taking the report should be recorded.

5. Breach of Data Security. In cases where the Identity Theft involves unauthorized access to unencrypted computerized data, the Program Manager will be notified and will determine whether additional reporting/notification steps must be taken under applicable law, including but not limited to HIPAA.

6. Notifying the Victim. After consulting with law enforcement about the timing and the content of any victim notification, the Program Manager, or his or her designee, shall determine whether notice to a suspected victim of Identity Theft is appropriate. Medical information pertaining to the suspected perpetrator of the Identity Theft will not be disclosed to the victim. Victims will be encouraged to complete an FTC Identity Theft Affidavit, to notify a consumer reporting agency, and to cooperate with law enforcement in the investigation and prosecution of the Identity Theft.

7. System Flags. ABI’s Program Protocols may provide for system’s flags to alert staff to potential Identity Theft.

8. HIPAA Compliance. The Program Manager shall determine whether as a result of the Identity Theft, protected health information was inappropriately disclosed. The Program Manager shall take steps to appropriately account for and mitigate the effects of any inappropriate disclosures in accordance with ABI’s HIPAA policies and any related business associate agreements.

9. Request for Transactions/Fair Credit Reporting Act. Victims of Identity Theft may have the right to request certain records of business transactions relating to services provided to persons who have committed Identity Theft. All such requests shall be forwarded to the Program Manager for evaluation in accordance with the Fair Credit Reporting Act and other applicable laws, including but not limited to the HIPAA privacy regulations. Without limiting the foregoing,

the person seeking the records must provide (i) proof of his or her identity; (ii) a copy of a police report relating to the Identity Theft; and (iii) a completed FTC Identity Theft Affidavit. The request may be denied if there is a good faith determination that the true identity of the person requesting the information cannot be verified, the request for information is based upon a misrepresentation, or state or federal law prohibits the requested disclosure. No protected health information of the person committing the Identity Theft (including but not limited to any information about the person's medical history, diagnosis, or services received) shall be provided to the victim.

10. No Action. If the Program Manager, or his/her designee, determines that no action is required in response to an incident of suspected or confirmed Identity Theft, the reasons for that determination shall be documented.

4824-9462-9380, v. 2