DeZavala-Shavano Veterinary Clinic

Information Security Program

Veterinary Practice
Employee Documents

(This page intentionally left blank)

SENSITIVE INFORMATION POLICY

PURPOSE

The Sensitive Information Policy provides guidelines for the safe and appropriate access to and protection of data and information collected, maintained or destroyed by the practice. This includes:

- Guidelines for determining what information is to be treated as sensitive
- Standards of protection for sensitive information
- Access control standards (who is allowed to see what) for sensitive information
- Standards for training and education, including content and frequency

SCOPE

This policy covers the appropriate access to and protection of paper and electronic information related to customers, employees, company Intellectual Property, information or data entrusted to this company by another organization (for use or for storage), and any other information so designated. Persons responsible for following this policy include employees, contractors, vendors, service providers, temporary or seasonal employees, volunteers and other individuals who have reason to be provided or gain access to covered sensitive information, hereafter referred to as "employees."

DETERMINING SENSITIVE INFORMATION

Sensitive information is any information that, if released, could be considered to represent a threat or risk to company employees or customers, the company itself, the company's reputation or the company's ability to conduct business. This includes, but is not limited to:

Personally Identifiable Information – This term includes any data point that may reasonably be considered, either singly or in combination, to individually identify a customer or employee, such that the information could potentially lead to Identity Theft.

- Name
- Address
- Social Security Number
- Drivers License Number
- Date of Birth
- Phone numbers
- Email address

Account Information – Any information that is used for or is the result of business transactions, financial or otherwise. This also includes customer history, to include details about products or

services rendered as part of such transaction.

Financial Information - Credit Card numbers, Bank Account details, Insurance Numbers, internal identifiers, customer/patient histories.

Company Information – Any information that might reasonably be considered to be proprietary data, company secrets, work products, or information that may be of substantive value to the company.

Other Information – Any information designated as sensitive by the Information Security Officer.

STANDARDS OF PROTECTION

Sensitive information is to be protected at all times. Only information which is vital to the conduct of company business or required by law shall be collected or maintained.

Hard copy information – Any sensitive information that is collected, maintained or stored on paper shall be kept under lock. Where possible, storage shall be in locked file cabinets. If this is not possible, any office or room where it is maintained shall be locked when unoccupied. When in use, information shall be kept in a folder or under a cover sheet. Information shall not be left unattended on desks or tables.

Electronic information – Company networks shall be maintained with appropriate security including, as appropriate, firewalls, anti-virus, anti-spyware, anti-spamware, passwords, and full-disk encryption. Any laptops shall be protected with encryption, when possible.

Information destruction –Sensitive information shall be properly destroyed when no longer required. CDs and DVDs shall be broken or rendered inoperable by an appropriate mechanical device. Hard copies shall be shredded by a certified vendor or in a cross-shredding device. Hard drives or data storage devices shall be rendered inoperable consistent with industry standards.

In the event that the company is bought or goes out of business, the Sensitive Information associated with customers and employees shall only be retained or used for the specific purpose of continuing existing relationships. Any other use of this information may only be made with the express consent of the individual.

ACCESS CONTROL STANDARDS

Access to sensitive information shall be limited to the greatest extent possible. Access to sensitive information shall be positively controlled and access shall be granted on either a job (role)-based or responsibility (individual) based profile. Scope of access to information shall be changed immediately upon any changes to positions or responsibilities. Employees shall be properly trained on the handling of sensitive information prior to being given access. As soon as

it is apparent that an employee will be separated from the company, all access to sensitive information shall be restricted.

TRAINING AND EDUCATION

Every employee shall be trained on the proper handling of sensitive information. This includes, but is not limited to the appropriate ways to collect, maintain and destroy sensitive information so as to minimize the chance of exposure.

To properly understand why sensitive information is treated so carefully, all employees shall be educated about the types of Identity Theft and how they can be affected. This education will enable employees to act appropriately, even when policy and practices are insufficient guidance in given situations, to protect themselves, the company and its customers.

Periodic refresher training shall be conducted as needed to ensure that this policy is maintained at the highest possible standard.

Completion of training and education shall be appropriately documented along with an agreement to follow company sensitive information protection requirements.

ENFORCEMENT

Periodic checks shall be conducted to ensure that this policy is being followed. This shall include, but is not limited to, walkthroughs, interviews and security checks.

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

ROLES AND RESPONSIBILITIES

The Information Security Officer (ISO) is responsible for ensuring that all are enforcing this policy and ensuring that the policy is updated on a periodic basis.

All employees are responsible for understanding and following this policy.

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Identity Theft Prevention Program

PURPOSE

The purpose of the Identity Theft Prevention Program, hereafter referred to as "ITPP," is to provide a framework for DeZavala-Shavano Veterinary Clinic to actively prevent and/or mitigate fraudulent transactions associated with Identity Theft. This is done by standard practices for authenticating customers or potential customers to be sure that they are who they say they are, or at the very least that they are the same person with whom a business relationship exists. As the crime of Identity Theft transforms, the authentication methods used to prevent this fraud will also evolve.

SCOPE AND COVERED ACCOUNTS

This policy covers all business, personal and household accounts, as well as any other accounts so designated, for which there is a reasonably foreseeable risk of identity theft or to the safety and/or soundness of the company from identity theft, including financial, operational, compliance, reputation, or litigation risks. Persons responsible for following this policy include full- and part-time employees, contractors, vendors, service providers, temporary or seasonal employees, volunteers and other individuals who have reason to be provided with or gain access to covered sensitive information. The following are examples of accounts covered under this policy:

- Client accounts
- Company accounts
- Employee accounts, including volunteers
- Vendor accounts
- Any other account directly related to the operation of the company as deemed appropriate

RED FLAGS

Red Flags are indicators of potentially fraudulent transactions. These may become noticeable as either the establishment of an account or as an attempt to conduct a transaction using an existing account. These Red Flags do not, in and of themselves, constitute proof of Identity Theft, but they should be considered as strong indicators warranting additional scrutiny and consideration before completing the transaction and/or opening the new client account.

The Red Flags will be evaluated on a yearly basis to determine their appropriateness and to determine if some should be removed and others should be added. Anyone working with any covered accounts has the responsibility to provide input regarding which Red Flags should be adopted and which provide the best indicators for stopping potential Identity Theft. The following Red Flags are currently in use as indicators of potentially fraudulent activity:

Alerts, Notifications or Warnings from outside organizations

- A fraud or active duty alert is active or has been previously active.
- A credit freeze is active or has been previously active.
- Information indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:
  - A recent and significant increase in the volume of credit or other inquiries
  - An unusual number of recently established credit relationships.
  - A material change in the use of credit, especially with respect to recently established credit relationships.
- An account that was closed for cause or identified for abuse of account privileges.
- Notification is otherwise provided that there has been fraudulent activity reported regarding the account.

Suspicious Documents

- Documents provided for identification appear to have been altered or forged.
- The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
- Other information on the identification is not consistent with information provided by the person opening a new account or customer presenting the identification.
- Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.
- An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.
- Name on check or credit card being presented for payment does not match the name on the client's account.
- Check payment is made with a temporary check.

Suspicious (Personal) Identifying Information

- Personal identifying information provided is inconsistent when compared against external information sources used by the company. For example:
  - The address does not match any address previously provided.
  - The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.
  - The registration information regarding the animal is inconsistent with provided information.
- Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.
- Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the company. For

example: the address on an application is the same as the address provided on a fraudulent application.

- Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:
  - The address on an application is fictitious, a mail drop, or a prison.
  - The phone number is invalid, or is associated with a pager or answering service.
  - The SSN provided is the same as that submitted by other persons opening an account or other customers.
  - The address or telephone number provided is the same as or similar to the account number or telephone number submitted by other persons opening accounts or other customers.
- The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
- Personal identifying information provided is not consistent with personal identifying information that is on file.
- For companies that use challenge questions (asking the client a question that only he/she would know), the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

Unusual Use of, or Suspicious Activity Related to, the Covered Account

- Shortly following the notice of a change of address for a covered account, the company receives a request for new, additional, or replacement of documents or account information or for the addition of authorized users on the account.
- A new account is used in a manner commonly associated with known patterns of fraud patterns. For example: the customer fails to make the first payment or makes an initial payment but no subsequent payments.
- A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:
  - Nonpayment when there is no history of late or missed payments; A material increase in the use of available credit.
  - A material change in purchasing or spending patterns.
  - An account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).
  - Client brings a pet in for services but indicates another person will be paying (and no prior agreement is on file for such a payment arrangement).
  - Client incurs a large bill or makes an unusually large payment, but does not have any or little prior payment history with the clinic.
- Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered

account.
- The company is notified that the customer is not receiving paper account statements.
- The company is notified of unauthorized charges or transactions in connection with a customer's account.

Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection with Accounts Held by the Company

- The company is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

AUTHENTICATION

With the knowledge of what to look for, employees participating in any way shall actively search for the appearance of any Red Flags. The following processes shall be used to establish that the customer is who he/she says he/she is and, where appropriate, that he/she is the person with whom an account is already established.

New Clients

A government-issued picture identification is to be requested when a person establishes a new account with the clinic. This is to ensure the physical description/picture matches the person requesting the new account as well as matches the name and address that the person has indicated on the New Client Form. If there is a discrepancy, an additional form of identification is to be requested such as a credit card, check, job/school/military identification, etc.

Existing Clients with Inactivity for 2 Years or More (or Otherwise in Question)

For clients who have a period of inactivity on their account for 2 years or more (or otherwise in question), the client is to be asked to verify the name, address and phone number on the account. If there is a discrepancy, the client is to be asked to provide previous information that may have been used in the past. If the previous information can be verified with what is on the client's clinic account, update the old information with the client's new information (i.e. moved--new address or phone number, marriage/divorce--new last name). If the person can not verify the previous information, a government-issued picture identification is to be requested.

Clients Making Payment Plan Arrangements

In the event a client is making payment plan arrangements by cash or hold check/credit card, a government-issued picture identification is to be requested to verify the physical description/picture matches the person requesting a payment plan as well as matches the name and address on the clinic account.

For hold check payments, the name and address on the picture identification must match the name and address on the hold check(s). For credit card hold payments, the name on the picture identification must match the name on the credit card. If there is a discrepancy, an additional form of identification is to be requested such as a check, job/school/military identification, etc.

When a client is applying for Care Credit financing, 2 (two) forms of identification are to be requested such as a driver's license, student/military identification, etc. to verify the physical description/picture matches the person applying for Care Credit as well as matches the name and address on the application.

Payment by Phone

For Care Credit or credit card payments made by phone (when the payer is unknown), the client is to be asked to verify the name, address and phone number on the account prior to processing the payment. If there is a discrepancy, the client is to be asked to provide previous information that may have been used in the past. If the previous information can be verified with what is on the client's clinic account, update the old information with the client's new information (i.e. moved--new address or phone number, marriage/divorce--new last name). If the person can not verify the current or previous information, then payment will not be able to be processed by phone, and the client will need to come into the clinic to make payment.

RESPONDING TO RED FLAGS

When Red Flags appear or are identified as associated with a transaction or an account, it is vital to act as quickly and prudently as possible to determine whether or not there has in fact been fraud committed or attempted and to then take the appropriate actions to respond.

The first response to the appearance of a Red Flag is to complete additional authentication steps. This may mean providing additional documentation to verify the identity of the individual or the pet or determining another form of payment to preclude any negative result if it is an attempt to commit fraud.

Additional steps may also be appropriate if these steps either confirm that the transaction is fraudulent or the Red Flag is not able to be otherwise resolved. These steps should be taken after consultation with a manager or the owner of the company.

- Cancel the transaction.
- Notify and cooperate with appropriate law enforcement.
- Determine extent of liability to company.

RESTORATION OF VICTIMS

In the event that an instance of Identity Theft is discovered, every reasonable effort will be made to notify the affected victim. This should include a summary of what occurred and any actions

taken to correct the problem.

Any erroneous information entered into the account records as a result of the Identity Theft shall be deleted or segregated into another record so as not to be interpreted as having been entered as part of the victim's record. Any assistance necessary shall be provided to Law Enforcement to assist in the correction of the problem.

PERIODIC UPDATES

Annually or as required, this policy shall be reviewed to determine the value and appropriateness of the Red Flags, authentication mechanisms, training, and other process components. Where required, the policy shall be adapted to reflect the current state of the business.

TRAINING AND EDUCATION

Prior to being asked to participate in customer transactions, each employee shall be trained on this policy and how to detect potential Red Flags. Refresher training shall be provided annually and/or in the event that an instance of Identity Theft is missed and subsequently discovered.

Training shall also be conducted for all employees in the event that substantive changes are made to this policy or how it is interpreted or implemented.

ROLES AND RESPONSIBILITIES

The Information Security Officer (ISO) is responsible for enforcing this policy and ensuring that all employees are properly trained and updated on this policy. He/she will also report on the effectiveness of this program to the Board of Directors or Senior Management should a Board of Directors not be in place.

All employees are required to implement this policy as consistent with their duties.