Policy updated: 13/06/2023

Credit Card Processing and Handling Security Policy

Client Complaints

Policy Statement
Think Grow connect must take all appropriate measures to protect credit card numbers used to make payments to the company.

Rationale
Credit card transactions have become the preferred method for making payments for telehealth appointments including telephone appointments and Zoom appointments.

Every business that accepts credit and debit card payments is required to store this information in a secure and safe place. Additionally, the Company's reputation would be seriously damaged by the exposure of credit or debit card numbers. Employees who work directly with credit card processing and documentation are required to review and sign this policy on an annual basis.

Applicability of the Policy
This policy applies to all Think Grow Connect employees who have access to credit or debit card numbers accepted for payments to the company.

Procedures

1. Access to Customer Credit Card Data
    - 1.1. Access is authorized only for Think Grow Connect personnel who are responsible for processing or facilitating credit card transactions. Only authorized Company personnel may process credit card transactions or have access to documentation related to credit card transactions.
    - 1.2. A copy of this policy must be read and signed by authorized personnel on initial employment and annually thereafter.
    - 1.3. Signed policies will be maintained by the practice manager.

2. Transmission of Credit Card Information
    - 2.1 Insecure (unencrypted) transmission of cardholder data is prohibited. Credit card numbers and cardholder data may not be emailed, faxed, or sent via any electronic messaging technologies such as instant messaging or chat.

3 Telephone Payments
    - 3.1 When recording credit card information for processing via a dial-up terminal, only cardholder name, account number, expiration date, zip code, and street address may be recorded. It is not permissible to record and store the three-digit security code (CVV2).
    - 3.2 Store transaction documentation and merchant receipt in a secure (locked) area.

4 Card Present Transactions (Point-of-Sale)
    - 4.1 Point-of-Sale devices must be inspected for tampering before the first use of the week.
    - 4.2 Provide a receipt to the customer.
    - 4.3 Store transaction documentation and merchant receipt in a secure (locked) area.
    - 4.4 Department supervisors must maintain a list of all POS devices and personnel authorized to use them.

5 Retention and Destruction of Cardholder Data
    - 5.1 Cardholder data should be retained in a secure location only as long as is necessary for business purposes

5.2 Cardholder data will be destroyed when no longer needed. Paper will be crosscut shredded. Electronic files will be destroyed in a manner appropriate to the media on which they are stored.

6 Processing Involving Third-Party Service Providers

6.1 personal details of the client will not be released to any third parties

7 Security Incident Reporting

7.1 In the event of suspected tampering or substitution of a Point-of-Sale device or computer belonging to the company, or suspected loss or theft documents or files containing cardholder data the police and clients should be notified straight away.

3/35 Grey Street
PO BOX 1741
TRARALGON VIC 3844
Ph: 03 5176 4374
admin@thinkgrowconnect.com.au