Policy No: D0457

CM

Security of Consumer Payment Card Information Policy Directive

Version No.: v1.0
Approval date: 08 December 2017

Government
of South Australia

SA Health

Contents

Security of Consumer Payment Card Information Policy Directive

1. Policy Statement

The intent of this policy directive is to ensure that consumer provided payment card information is protected in compliance with the *Payment Card Industry Data Security Standards* (PCIDSS), Treasurer's Instruction *2 Financial Management,* and 28 *Financial Management Compliance Program*.

2. Roles and Responsibilities

This policy directive applies to all SA Health staff responsible in the management and receiving of consumer electronic payments for services provided by SA Health to its consumers.

2.1. Delegated Managers

Managers who have the responsibility for receiving information for, and/or processing, payment card transactions must:

- ensure ongoing compliance with PCIDSS
- ensure revenue officers are provided with ongoing training to meet PCIDSS requirements
- ensure the PCIDSS Self-Assessment Questionnaire (SAQ) is completed and returned in accordance with the bank's requirements
- advise Corporate Support of non-compliance issues in a timely manner, and
- work with Corporate Support and the bank to rectify any PCIDSS non-compliance.

2.2. Cashiers and Revenue Officers

Cashier and revenue officers are responsible for ensuring:

- ongoing compliance with PCIDSS
- all EFTPOS terminals are under supervision at all times
- all EFTPOS terminals are secured away during non-business hours, and
- all remittances and telephone messages containing payment card information are correctly disposed of at the close of each business day.

2.3. Corporate Support

Corporate Support team are responsible for:

- providing ongoing support to the business to ensure PCIDSS compliance,
- liaising with the bank on remedial solutions for non-compliance issues, and
- regularly reviewing the remedial action being undertaken by the business unit, to ensure PCIDSS compliance is achieved in a timely manner.

3. Policy Requirements

SA Health provides consumers with various payment options, and the use of credit/debit card payments is a convenient and often popular choice. With the acceptance of credit/debit card payments, responsibility to protect sensitive cardholder information, and to avoid card misuse and financial fraud, is required. The PCIDSS Council has established standards which SA Health must comply with, to ensure the storing, processing, and/or transmitting of confidential cardholder data is protected and secured.

3.1. Payment card information (PCI) requirements

PCI is received by revenue staff on a daily basis as remittance via internet, mail, phone, or in person. Only authorised people can have access to the cardholder's PCI. The business must not accept PCI via email.

Sending cardholder's PCI **must not** be done via email or other media devices under any circumstance, as there is no assurance that the information will remain secure.

3.1.1. Storage

Paper and electronic storage of PCI must be kept to a minimum, and stored in a secure area that can be tracked from the time it is received, through to time of the eventual destruction of the cardholder's PCI.

Unless there is a legitimate business need, with prior authorisation from the cardholder, PCI must not be retained.

Merchant copies of receipts may be retained in secured storage (e.g. locked filing compactors/cabinets), as evidence of the transaction for up to five years (*General Disposals Schedule No. 30*), and the cardholder's authentication details must be truncated.

3.1.2. Destruction

Prior to destruction, all paper and electronic forms of cardholder's PCI must be appropriately secured. All cardholders' PCI that is stored by way of paper or in electronic form (eg telephone messages (written or recorded) containing any payment card details) must be correctly disposed of by the close of business each day, with only the merchant copy of the receipt retained as evidence of the transaction.

In accordance with PCIDSS:

- staff must not dispose of PCI paperwork by ripping up the information and placing the pieces in a general bin
- all paper forms of PCI must be securely disposed of appropriately (eg approved confidential waste management bin, or destruction by pulping, or cross shredding etc.), and
- all electronic PCI must be deleted from network drives and other storage devices ensuring the data is unrecoverable.

3.1.3. EFTPOS terminals

Cashiers and revenue officers must ensure that only authorised staff have access to the electronic funds transfer at point of sale (EFTPOS) terminals and that all EFTPOS terminals are secure and under supervision during operating hours. During non-business hours EFTPOS terminals must be secured away to avoid unauthorised access.

Managers must notify SA Health's banking provider (the bank) immediately if:

- the EFTPOS terminal is missing
- the EFTPOS terminal appears damaged or shows signs of having been tampered
- the EFTPOS terminal prints incorrect or incomplete details, and
- an approach has been made by someone seeking to perform maintenance, remove or swap the terminal – without prior notification from the bank.

At no time should a physical payment card (with cardholder's PCI, containing a magnetic strip or equivalent data on a chip) be retained on site. Where a payment card is found, the card must be kept secured while revenue officers attempt to contact the cardholder. Refer to the *Security of Consumer Payment Card Information Procedure* for further details regarding security, storage and disposal of PCI.

3.2. Compliance assessment

SA Health's banker, in collaboration with the PCIDSS Council, manages the Self-Assessment Questionnaire (SAQ) process, which assesses the business unit's compliance to the standards. On an ad-hoc basis, the bank will determine who and when a SAQ must be completed, and will liaise with Manager, Corporate Support. Corporate Support will work collaboratively with the pertinent business unit's Chief Finance Officer to ensure the SAQ is completed. Delegated managers must complete the questionnaire within the timeframe set by the bank.

If the self-assessment process discovers non-compliance, remedial action must be undertaken immediately, as per the bank's advice. In these instances, the Manager, Corporate Support must be made aware of what areas are non-compliant and what action will be taken to rectify it. The Manager, Corporate Support will follow up with the business unit until all remedial action has been resolved.

Non-compliance may incur fines, or the revoking of all merchant card facilities.

3.3. Training

Each staff member who receives consumer electronic payments on behalf of SA Health must be adequately trained in the requirements of PCIDSS, the handling of payment card information and the compliance mechanisms which ensure that sensitive data is managed appropriately. It is the responsibility of managers to ensure staff are appropriately trained prior to receiving electronic payments.

4. Implementation and Monitoring

Evaluation of this policy directive will be assessed when all PCIDSS requirements are met and all cardholder details are correctly stored and destroyed. Monitoring is undertaken by the bank using the SAQ, when it requests businesses to complete and return the SAQ in a timely manner, and where it identifies nil non-compliance issues. Where any non-compliance issues are identified, remedial action must be undertaken in accordance with the bank's requirements. Corporate Support will monitor and assist until all remedial action has been resolved.

Where non-compliance with this policy directive occurs, this may result in financial penalties being passed on by the PCIDSS Council regulator, and the revoking of all SA Health merchant card facilities. Further, the risk of cardholders' information not being correctly stored and banking details obtained could result in the conduct of fraudulent activity. The loss of consumer card data, and subsequent misuse, may lead to adverse media coverage and potential reputational damage; undermining consumer confidence with SA Health.

5. National Safety and Quality Health Services Standards

N/A

6. Definitions

In the context of this document:

- **business unit** is a collective term which encompasses the operating units within the Local Health Networks (LHN), Department for Health and Ageing (DHA), and SA Ambulance Service (SAAS). Business Units may be used to describe an individual hospital within a LHN (eg RAH), as well as a Division within DHA (eg eHealth Systems), or clinical area within a LHN (e.g. cardiology).
- **EFTPOS** (electronic funds transfer at point of sale) is an electronic payment system involving electronic funds transfers based on the use of payment cards, such as debit or credit cards, at payment terminals located at health sites.
- **managers,** in the context of this document, are all supervisors and managers with responsibility for an area which receives information for, and / or processes payment card transactions.
- **Payment card** is a device that enables its owner (the cardholder) to make a payment by electronic funds transfer. Payment cards, commonly called credit cards and debit cards, are usually embossed plastic cards.
- **Payment card information (PCI)** includes the full primary account number (PAN), cardholder name, expiration date and service code.
- **Payment Card Industry Data Security Standard (PCIDSS)** are technical and operational requirements set by the Payment Card Industry Council to protect cardholder data. The standards apply to all businesses that handle credit and debit payments, regardless of the size or number of transactions processed.
- **Payment Card Industry Data Security Standard (PCIDSS) Self-Assessment Questionnaire** is a validation tool banking provider issue to business units to complete and return. On assessment, and if necessary, remediation action may be provided to obtain compliance.
- **SA Health** is the corporate identity, and not the legal entity, for all the Local Health Networks, SA Ambulance Service and the Department for Health and Ageing.

7. Associated Policy Directive/Policy Guidelines and Resources

- *Payment Card Industry Data Security Standard*
- *SA General Disposal Schedule No. 30 - State Government Agencies in South Australia 2016*
- *Security of Consumer Payment Card Information Procedure*
- Treasurer's Instruction 2 *Financial Management*
- Treasurer's Instruction 28 *Financial Management Compliance Program*

8. Document Ownership and History

Document developed by: Policy and Compliance Corporate Finance Services, Finance
File / Objective No.: 2017-08892 | qA449256 | CM-P1012
Next review due: 31 October 2020
Policy history: Is this a new policy? **N**
Does this policy amend or update and existing policy? **N**
Does this policy replace another policy with a different title? **Y**
If so, which policy (title)? *Payment Card Industry Data Security Standards (PCIDSS) Compliance*

Approval Date	Version	Who approved New/Revised Version	Reason for Change
08/12/2017	V1.0	SA Health Policy Committee	Original approved version published
24/07/17	V0.1	Director, Corporate Finance Services	Original published on Oracle Assist