

Payment Card Handling at WakeMed

PCI DSS Overview

Course Objectives

- Gain an understanding of the Payment Card Industry Data Security Standards (PCI DSS)
- Review responsibilities related to accepting in-person payment card transactions
- Review responsibilities related to accepting card-not-present payment card transactions

What is PCI DSS?

- The Payment Card Industry Data Security Standard (PCI DSS) is a set of security requirements that merchants like WakeMed are contractually obligated to comply with in order to accept debit and credit cards (a.k.a. “payment cards”).
- The scope of PCI DSS covers the people, process, and technology that interact with cardholder data.

Cardholder Data

Cardholder data includes the Primary Account Number (PAN) by itself or in combination with a data element on a payment card.



Your Responsibility for Compliance

- All employees that interact with payment cards are required to be trained on applicable security procedures.
- Payment card handlers, like yourself, are our first line of defense to help maintain compliance and protect our customer's credit from fraud.

Card-Present Transactions

Card Present Payment Channels

- Card Present Transactions include any instance where the cardholder and their card are physically present to complete a transaction.
- The following are approved payment channels to accept card present transactions:
 - Ingenico ISC250
- Other devices or Point-of-Sale systems not mentioned in this training are not approved for taking card present credit card payments.
- ***Under no circumstances*** should cardholder data be written down for card present transactions. If devices are not working, follow your downtime procedures.



- Ingenico ISC250 point of sale devices are used for all patient facing credit card transactions.

Device Overview

Inventory of Devices

WakeMed maintains a list of devices that includes at a minimum:

- Make, model of device
- Location of device
- Device serial number
- Information Services and Patient Financial Services are responsible for reviewing and updating their inventory annually.

Device Maintenance

- Maintenance requests for POS devices are to be submitted to Information Services by submitting a Service Desk Ticket via Service Now.
- Once maintenance requests are approved, Information Services will provide the following details to the requesting individual:
 - Date maintenance will be performed
 - Name of individual that will perform maintenance
- Identity of the individual performing maintenance must be verified by the staff member requesting the service prior to granting them access to modify or troubleshoot devices.

Identifying Suspicious Activity

- Staff should be aware of suspicious behavior around POS devices. Examples include:
 - Attempts by unknown persons to steal, replace, unplug or open devices
 - Presence of card skimmers or other recording devices like cameras
 - Staff are responsible for performing physical inspections of all assigned POS devices to identify tampering or replacement. Staff are to document the POS device inspection on a signoff sheet and management is to review and signoff to indicate these procedures have been completed.
-

Inspection Guidance for POS Devices

- Regular inspections will help to detect tampering or replacement of a device, and thereby minimize the potential impact of using fraudulent devices.
- Examples of inspection techniques include:
 - Examine the POS device for the presence of card skimmers or other recording devices like cameras.
 - Photographs of approved POS devices that are known to be secure can be used to compare a device's current appearance with its original appearance to see whether it has changed.
 - Inspect the device serial number to ensure it has not changed.
 - Use a secure marker pen, such as a UV light marker, to mark device surfaces and device openings so any tampering or replacement will be apparent. Criminals will often replace the outer casing of a device to hide their tampering, and these methods may help to detect such activities.

Example of a POS skimming device

This skimmer was made to fit over the top of, or piggyback on, the real card reader.

In order for the overlay to fit atop the POS [point-of-sale] terminal, it must be longer and wider than the target device. For this reason, the case overlay will appear noticeably larger than the actual POS terminal. This is the primary identifying characteristic of this skimming device.

Skimmer

Actual POS device



Reporting Suspicious Activity

- Staff suspecting any sort of suspicious activity should report said activity immediately.
- Suspicious activity should be reported to:
 - Your department manager
 - Information Security
 - Internal Audit
 - If warranted, to WakeMed Campus Police

Card-Not-Present Transactions

Card-not-Present Payment Channels

- Card-not-Present transactions are any instance where cardholder data is received through approved payment channels and the cardholder and card are NOT physically present.
- The following are approved payment channels to accept card-not-present transactions:
 - IDTECH M130
 - Phone
- The following are examples of payment channels that are NOT approved for card-not-present transactions:
 - Email
 - Instant Messaging (e.g. Skype, Whatsapp)
 - Mail
 - Fax



WakeMed

Device Overview

IDTECH M130 point of sale devices
are used for all non-patient facing
credit card transactions.



Phone Transactions

- The following locations are the only approved locations to accept cardholder data by phone:
 - Revenue Cycle – Financial Clearance, Customer Service
 - Pharmacy
 - Birth and Family Education
 - Heart Center Inn
- New instances of accepting cardholder data by phone must be approved by the VP of Finance.

Phone Transaction Security

- Enter data directly into IDTECH POS device
- Do not write down cardholder data
- Do not ask for CVV if not needed for processing

Cardholder Data Disposal

All cardholder data must be disposed of following the Payment Card Industry Data Security Standard (PCI-DSS) Data Retention and Disposal Policy

Exception Handling Procedures

- An exception would be an instance where cardholder data is received or sent through an unauthorized channel (e.g. email)
- If you receive cardholder data through an unauthorized channel you should inform the sender of approved payment channels.
- All exceptions are to be reported to your department management

Training Assessment

Thank you for reviewing WakeMed PCI Training.
Please complete the competency assessment.
You must score an 80% to pass the test.

Cary Hospital

WakeMed PCI Training Assessment for Cary