

Corporate Policy

Payment Card Industry Data Security Standard (PCI DSS) Compliance Policy

Policy Purpose:

This policy outlines the responsibilities of The Ottawa Hospital (TOH) staff (defined below) who are involved in transmitting, storing, or processing payment card data. It provides information about the appropriate use of payment cards, our responsibility to prevent loss or fraudulent use of payment card data and sets out internal controls for creating and administering merchant accounts (defined below) at TOH.

Using payment cards to pay hospital accounts can be convenient for our patients and other clients. To continue accepting payment cards, TOH must comply with the requirements of the Payment Card Industry Data Security Standard (PCI DSS). The purpose of the PCI DSS is to protect cardholder data, specifically, to prevent loss or disclosure of customer information including credit card numbers. Cardholder data is protected through processes and controls designed to enhance payment card data security around the collection, use, storage, and handling of payment card information data.

Non-compliance with PCI DSS requirements exposes TOH to risks including loss of payment card acceptance privileges, increased processing fees, liability for damages, reputational damage, higher insurance costs and lost revenue and downtime for systems that are breached.

Scope:

This policy applies to all TOH staff as defined below and all TOH devices, systems, and networks involved in transmitting, storing, or processing Cardholder Data (defined below) at or on behalf of TOH.

This policy also applies to staff with teleworking arrangements and their remote work environments.

Definitions:

Cardholder Data: Any personal information (PI) associated with a person who has a credit or debit card (payment card). Cardholder Data includes the primary account number (PAN), which consists of a customer's 16-digit payment card number along with any of the following data: cardholder name, expiration date, card verification value, EMV chip data and mag stripe data. For the purposes of this policy Cardholder Data refers to payment card data only and not health card data as an example. Cardholder Data is classified as confidential under TOH's Information Classification model.

Epic: A health information system (HIS) that collects, stores, manages and transmits patient's electronic medical record (EMR) and supports hospital's operational management, including activities of health care providers.

Information System Assets: For the purpose of this policy, Information System assets include components of a point of interaction (see POI below), components of points of sale, networks used to transmit credit card information, and application used to transmit or process payments.

Just Culture: A framework used to ensure consistency in how breaches of duty are addressed in a supportive, just and ethical environment. The Just Culture supports honest reporting of breaches of duty with the goal of continuous improvement in the organization.

Merchant Department Most Responsible Person (MD MRP): The Director responsible for the department accepting payment cards. The Director has primary authority and responsibility for payment card transaction processing and/or third-party Service Providers accepting payment cards on behalf of TOH. For a full list of the MD MRP's responsibilities, see TOH PCI DSS Compliance Program and Payment Card Acceptance Procedure Manual.

Merchant: Any entity that accepts payment cards bearing the logos of any of the five members of PCI SSC (American Express, Discover, JCB, MasterCard or Visa).

Merchant Account: A type of business bank account that allows a business to accept and process electronic payment card transactions.

PCI DSS (Payment Card Industry Data Security Standards): A set of controls, processes, and other technical and operational requirements designed by the PCI Security Standards Council regarding the collection, use, transmission, storage, and handling of payment card data designed to protect cardholder data. These requirements have been agreed upon by the five major credit card companies and apply to all transactions surrounding the payment card industry and the merchants/organizations that accept these cards as forms of payment.

PAN: Primary Account Number is a key piece of cardholder data you are obligated to protect under the PCI DSS. Storing customers' full PAN data exponentially increases TOH's security risk and scope of compliance. Masking (a method of concealing a segment of data when displayed or printed) the PAN is a good method to prevent unauthorized use of the data when there is no business need to view the number.

Payment card: Debit or credit card issued by a qualified financial institution that allows its user to obtain money or to make a payment.

Personal Information (PI): Any information about an identifiable individual such as demographics, credit card information, employment history, etc. PI may be about TOH staff, volunteers, donors, or any other individual that entrusts information about themselves to TOH. PI can include information in many forms such as physical or electronic files, as well as audio, images, video footage, etc.

Point of Interaction (POI) is the initial point where data is read from a card. An electronic transaction acceptance product, a POI consists of hardware and software and is hosted in acceptance equipment to enable a cardholder to perform a card transaction. The POI may be attended or unattended. POI transactions are typically integrated circuit (chip) and/or magnetic-stripe card-based payment transactions.

Point of Sale (POS) is hardware and/or software used to process payment card transactions at merchant locations.

PIN Entry Device (PED) is a terminal that allows entry of a customer's personal identification number (PIN).

Telework or remote work: An arrangement that allows the employee to work in a location that TOH does not own or maintain.

Third-Party Vendor (also called "third-party service provider"): Business entities directly involved in transmitting, processing, or storing of Cardholder Data or which provide services that control or could impact the security of Cardholder Data.

Staff: Anyone who works on behalf of TOH. This includes permanent or temporary, full-time, part-time, casual or contract employees, trainees and volunteers, and vendors. This also includes administrative and clinical personnel like administrative assistants, physicians, residents, interns, researchers, and students, and any other individuals who perform work or supply services at TOH.

For a full list of PCI DSS related definitions, see [PCI Compliance Program site](#).

Policy Statement(s):

General

1. We are committed to safeguarding PI conveyed in processing payment card payments. In addition to complying with Corporate Policy – Privacy and related standard operating procedures when collecting, using, or disclosing PI, we will comply with PCI DSS and use secure methods to process payment card transactions.
2. We will not collect, transmit or store Cardholder Data in any electronic or physical form. This includes but is not limited to electronic files stored on SharePoint, OneDrive, Outlook, user notes in Epic or Enterprise Resource Planning (ERP) system, emails, or paper forms.

Merchant Accounts

1. We will only establish merchant accounts using TOH's approved service providers. We will not enter other payment arrangements with non-approved service provider(s) when collecting payment for TOH (e.g., PayPal, Square, Apple Pay, Shopify Payments, etc.).
2. If we need a merchant account to accept payment cards, our department is responsible for the costs of establishing the account. These costs may include: renting point-of-sale (POS) terminals, set-up and maintenance of a PCI terminal, installing cables for connectivity (if required), transaction fees, and costs associated with online e-commerce applications, payment applications, and service providers.
3. If we have a justified business need to accept payment cards, our Director or EVP may request a merchant account from the Director of Revenue and Accounts Receivable. We may only accept payments through a merchant account that has been established and

approved by the Director of Revenue and Accounts Receivable in Finance. The process to establish, modify, and close a merchant account can be found in the TOH PCI DSS Compliance Program and Payment Card Acceptance Procedure Manual.

4. Any physician or practice plan operating their own merchant account using the TOH network must demonstrate PCI DSS compliance and receive approval from Director of Revenue and Accounts Receivable before processing payment card data.
5. If we, or our information system assets, are involved in accepting, capturing, storing, transmitting, and/or processing payment card data (including systems that can impact the security of payment card data), we will comply with the current PCI DSS requirements to ensure the security of payment cardholder information. List of current PCI DSS requirements can be found in the TOH PCI DSS Compliance Program and Payment Card Acceptance Procedure Manual.
6. We will demonstrate PCI DSS compliance and receive approval from Finance (Revenue and Accounts Receivable) PCI Coordinator before processing payment card data, including by completing annual PCI DSS Compliance training.
7. All third-party service providers used for accepting, capturing, storing, transmitting, and/or processing payment card data must demonstrate PCI compliance by providing an annual Attestation/Statement of Compliance to PCI Coordinator. We will do our best to ensure that contracts with service providers minimize TOH's risk and clearly identify mutual responsibilities for PCI compliance.

Teleworking Arrangements

1. If we are teleworking and are involved with accepting, capturing, storing, transmitting, or processing payment card data, then we must comply with and must make sure our systems comply with current PCI DSS requirements.
2. Teleworkers will complete PCI Working From Home (WFH) Training prior to being given access to Cardholder Data and will repeat this training annually.
3. All payment applications, solutions and/or devices used for the acceptance, capture, storage, transmission, and/or processing of payment card data must comply with the latest version of PCI DSS.

Exemptions to this policy

1. Any staff who cannot comply with this policy must contact Director, Revenue and Accounts Receivable in Finance who will consider whether an exemption is possible or appropriate.

Responsibilities

1. All TOH staff and departments involved in accepting, capturing, storing, transmitting, or processing payment cards (including through management/oversight roles) are responsible for complying with this policy.
2. Any TOH staff working from home while involved in the acceptance, capture, storage, transmission and/or processing of payment cards, is responsible for knowing and adhering to TOH security policies and procedures, including limiting access to cardholder data within their WFH environments and securing network and computer equipment used at home for work purposes.
3. Additional responsibilities are outlined in the TOH PCI DSS Compliance Program and Payment Card Acceptance Procedure Manual.

Oversight

1. Finance's Revenue and Accounts Receivable Team will oversee the enforcement of this policy and associated procedures.
2. The PCI Coordinator (who is a member of the Revenue and Accounts Receivable Team) is responsible for approving or facilitating additional approvals if required, all new merchant accounts and any changes requested to existing merchant accounts.
3. Decisions to suspend or revoke a merchant account will be made by the Director of Revenue and Accounts Receivable in Finance.

Compliance with Policy

1. Any breach, or a suspected breach of this policy must be reported following procedures outlined in TOH Payment Card Acceptance Procedure Manual. Any breach or suspected breach of this policy which has also resulted in a breach or suspected breach of privacy must be reported as outlined in Corporate Policy – Privacy.
2. Any failure by a unit or a department to comply with this policy may result in suspension or revocation of their merchant account.
3. Staff who do not comply with this policy may face a Just Culture investigation as outlined in Corporate Policy – Employee Accountability and may have their working from home agreement suspended or revoked.

Related Documents:

TOH PCI DSS Compliance Program and Payment Card Acceptance Procedures Manual

TOH POS Security Training and Procedures

[TOH Information Systems Asset Management Policy](#)

[Corporate Standard Operating Procedure – Retention and Destruction of Corporate Records by Record Type](#)

[Corporate Policy – Privacy](#)

[Corporate Standard Operating Procedure – Consent to Collection, Use and Disclosure of Personal Information or Personal Health Information](#)

[Corporate Standard Operating Procedure – Privacy Breach Management](#)

[Corporate Standard Operating Procedure – Privacy and Security Training](#)

[Corporate Policy – Telework and/or Flexible Work Arrangements](#)

[Corporate Policy – Employee Accountability](#)

Related Legislation or Regulatory Requirements:

Payment Card Industry Data Security Standard - PCI Security Standards Council
<https://www.pcisecuritystandards.org>

References:

Payment Card Acceptance Policy
<https://www.queensu.ca/secretariat/policies/finance/payment-card-acceptance-policy>

Rollins Finance PCI DSS Policy
www.rollins.edu/finance/documents/PCI-policy.pdf

Cuny Payment Card Industry (PCI) Compliance Policy
<https://www.cuny.edu/wp-content/uploads/sites/4/page-assets/about/administration/offices/budget-and-finance/resources/finance-professionals/CUNY-Payment-Card-Industry-PCI-Compliance-Policy-Final-March-2021.pdf>