


<b>Name of Policy:</b>	Payment Processing and Cash Handling	 <p><b>Effective Date:</b> 03/24/2021</p> <p><b>Initial Effective Date:</b> 03/01/2017</p>
<b>Policy Number :</b>	3364-132-29	
<b>Department:</b>	Patient Access	
<b>Approving Officer:</b>	Chief Financial Officer	
<b>Responsible Agent:</b>	Director, Patient Access	
<b>Scope:</b>	Patient Access	
<input type="checkbox"/> New policy proposal <input type="checkbox"/> Minor/technical revision of existing policy <input checked="" type="checkbox"/> Major revision of existing policy <input type="checkbox"/> Reaffirmation of existing policy		

**A. Policy Statement**

The University of Toledo Medical Center (UTMC) has controls and procedures to standardize cash handling and assure PCI (payment card industry) compliance to securely collect, store and deposit funds. This policy addresses PCI compliance, cash handling, and deposit procedures.

**B. Purpose of Policy**

The UTMC Patient Access Department establishes the protocol for cash handling. All Point of Service employees with cash handling responsibilities are given clear direction to properly and safely perform their job duties. It is also necessary to outline and use methods to ensure PCI compliance and timely deposits.

**C. Scope**

This applies to all UTMC Point of Service employees handling payments from patients, as well as those required to log PCI compliance.

**D. Procedure**

**a. PCI Compliance**

- i. All registration areas will maintain and update a current device inventory list utilizing the Device Inspection Log (An electronic copy of the device inspection log can be found in the department Z drive). The device inspection logs will be appropriately saved by management.
  - a. Make and model number
  - b. Location of device
  - c. Serial number or another unique identifier
- ii. Physical inspections of devices must be conducted once weekly for potential tampering or substitution. The following will be included during inspections and documented on the Device Inspection Log
  - a. Is the device in the designated location?
  - b. Is the color and condition of the device as expected, with no additional marks or scratches?
  - c. Are parts of the card reader loose? Or does anything move or wiggle when pulled on?
  - d. Are there any loose or missing screws?
  - e. Are the security seals and labels present with no signs of peeling or tampering?
  - f. Is the number of connections to the device as expected, with the same type and color of cables?

- g. Is the pin pad thicker than normal?
    - h. Are there any unauthorized electronic devices (phones, iPods, etc.) near the device?
    - i. If tampering/substitution is suspected, please report immediately to direct supervisor and the University of Toledo IT department
  - iii. IT security policies pertaining to responsible use, safeguards, asset management, devices and workstations, disaster readiness and incident response can be accessed by visiting: [https://www.utoledo.edu/policies/administration/info\\_tech/](https://www.utoledo.edu/policies/administration/info_tech/)
  - iv. The Patient Access Manager/Supervisor will restrict access to cardholder data as follows:
    - a. When assigning user ID's, the least privileges necessary will be granted to ensure performance of necessary job duties
    - b. Will be assigned to only those roles that specifically require privileged access
  - v. The Patient Access Manager will notify IT of any employee who has been terminated or who is no longer employed in the department.
  - vi. Each location has appropriate facility entry controls in place to limit and monitor physical access to systems in the cardholder data environment to include authorized personnel only. Those include but are not limited to:
    - a. Badge readers
    - b. Pin pads
    - c. Door locks
    - d. Cameras
    - e. Other control mechanisms
  - vii. The Patient Access Manager is responsible for ensuring that all media is physically secured, classified so the data sensitivity can be determined, and media is properly destroyed. This includes but is not limited to:
    - a. Computers
    - b. Removable electronic media
    - c. Paper receipts
    - d. Paper reports
    - e. Faxes
- b. Cash Box
- i. Cash boxes are in each Point of Service area and are established with a set amount to be maintained at all times.
    - a. See Appendix A for cash box totals.
  - ii. Two Point of Service staff members will count the contents of the cash box and co-sign totals twice daily once in the AM and once in the PM using the Reconciliation log (Appendix B).
    - a. In the morning, the first two staff members on duty will complete the first cash box count of the day.
    - b. In the afternoon, the last two staff members on duty will complete the second cash box count of the day.
    - c. Cash boxes will be locked and stored in a locked drawer when not in use.
  - iii. The main bank will maintain a balance of amount noted in Appendix A.
    - a. The main bank will have limited access to Patient Access leadership and designated Patient Access employees.
    - b. The main bank is to be utilized only by authorized patient access employees to make change.
    - c. The main bank will be counted before and after each exchange.
    - d. The main bank will be in the Main Lobby safe.

iv. In the event of a cash box or main bank discrepancy, the following procedure will be followed:

- a. The discrepancy will be reported to Point of Service Manager by email and phone call immediately upon discovery.
- b. Point of Service Manager will investigate the events surrounding the discrepancy and report to the Director a summary of investigation to determine if next steps are necessary.
- c. Cash box discrepancy will be filled by the main bank.
- d. The investigation form (Appendix C) will be utilized during the investigation process.
- e. The completed investigation form and daily Reconciliation log copies will be submitted to leadership and stored in the department Z drive.

v. Internal audit will conduct random audits of cash boxes and the main bank.

c. Deposits

- i. Registration is expected to reconcile and drop all cash, applicable checks, and receipts in the safe located in their area each day by the end of their shift.
- ii. Registration leads, supervisor or manager will collect all deposits from safe twice a week.
  - a. Cash/checks are securely transported in a discrete manner.
- iii. A cash reconciliation and deposit are completed twice a week by a minimum of two people (i.e., lead registration and/or management).
  - b. This process must be done in a secure office with a closed door.
  - c. Cash/checks will be counted, and a deposit will be created, including a deposit slip, and put into a sealed bank bag.
  - d. Deposit will be locked in a safe and picked up by the bank

E. References

- a. Appendix A: Cash Box Totals
- b. Appendix B: Daily Reconciliation Log
- c. Appendix C: Investigation Form
- d. Appendix D: Device Inspection Log

<p><b>Approved by:</b></p> <p><u>/s/</u> _____ <u>03/24/2021</u> Laura Kern Date Director, Patient Access</p> <p><u>/s/</u> _____ <u>03/24/2021</u> Troy Holmes Date Chief Financial Officer</p> <p><i>Review/Revision Completed By:</i> Laura Kern</p>	<p><b>Review/Revision Date:</b></p> <p>03/01/2017 07/01/2019 03/24/2021</p> <hr/> <p><b>Next Review Date:</b> 07/01/2022</p>
<p><b>Policies Superseded by This Policy:</b></p>	

*It is the responsibility of the reader to verify with the responsible agent that this is the most current version of the policy.*

## Appendix A: Cash Box Totals

POS Location	
Ruppert	\$325
HVC	\$225
Main Lobby	\$225
Medical Pavilion	\$325
SC / SWR	\$275
George Isaac	\$225
CCC	\$300
ER	\$275
Main Bank	\$1,300
Total	\$3,200



Appendix C: Investigation Form

---

Name of Investigator \_\_\_\_\_ Date of Investigation \_\_\_\_\_

Location \_\_\_\_\_

Date and Time of Discrepancy \_\_\_\_\_

Staff Present in Location on Date of Discrepancy (include shift worked):	

Staff with Access to Cash Box and/or payment device:	

Added Information:

---

---

---

---

---

---

---

---

---

---

---

\*Note: A copy of the daily recon log for the previous five business days must be included with this form.

