TITLE: **PAYMENT CARD INDUSTRY CARDHOLDER DATA HANDLING POLICY**

PURPOSE: To properly secure and manage cardholder data.

POLICY STATEMENT:

Harris Health System (Harris Health) Information Security and the Office of Corporate Compliance (OCC) will oversee the development, implementation, and management of Harris Health Payment Card Industry (PCI) policies, procedures, and practices in accordance with the PCI Data Security Standards.

POLICY ELABORATIONS:

This policy provides overall guidance for the consistent protection of cardholder data, and applies to all users of Harris Health's cardholder data systems that store, process, or transmit cardholder data.

I. DEFINITIONS:

A. **CARDHOLDER DATA:** Cardholder Data consists of at least the full primary account number (PAN). Cardholder Data may also appear in the form of the full PAN plus any of the following:

1. Cardholder name;
2. Expiration date;
3. Service code.

B. **DISCLOSURE:** The release, transfer, provision of, access to, or divulging in any manner Cardholder Data outside of Harris Health.

C. **INFORMATION SYSTEM:** Any telecommunications and/or computer related equipment or interconnected system or subsystems of equipment used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data (digital or analog); including software, firmware, and hardware.

D. **INFORMATION USER:** Any person who reads, enters, processes, swipes, updates, sends, copies, prints, or otherwise uses or accesses Cardholder Data.

E. **PRIMARY ACCOUNT NUMBER (PAN):** A unique payment card number that identifies the card issuer and the unique cardholder account. This number is either fifteen (15) or sixteen (16) digits long.

F. **RISK:** A factor, event, element, or course of action that exposes Harris Health to potential liability, financial loss, and/or data loss.

G. **SENSITIVE AUTHENTICATION DATA** (SAD): Security-related information including but not limited to card validation codes/values, full magnetic-strip data, personal identification numbers (PIN), used to authenticate and/or authorize cardholders' payment card transactions.

II. CARDHOLDER DATA:

Cardholder Data, regardless of form (e.g. print, website, recording, e-mail, document, input data, and output data) refers to:

A. Credit card number, which is also known as a Primary Account Number (PAN). The numbers within the outlined box in Figure 1 represent a PAN.

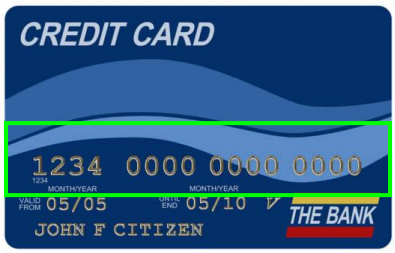

Figure 1: Primary Account Number

B. In conjunction with the PAN, the following elements are considered Cardholder Data:

1. Cardholder name;
2. Account expiration date; and
3. Security code

In addition to Cardholder Data, SAD includes the full contents of a card track (from the magnetic strip located on the back of a card, equivalent data on a chip, or elsewhere), the PIN known only to the cardholder, and/or the card validation code shown in Figure 2:

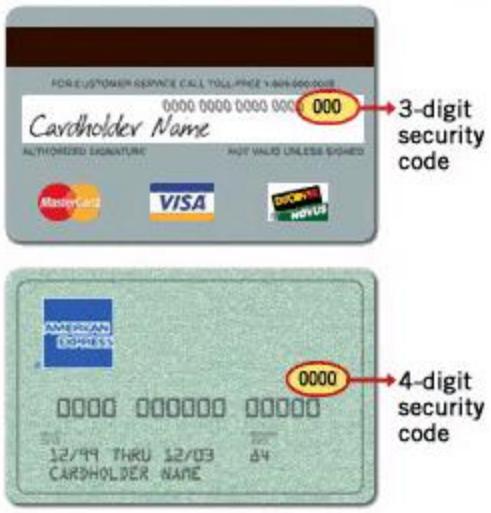

Figure 2: Card Validation Code

SAD should never be stored after authorization of a payment transaction even if encrypted.

III. PCI CARDHOLDER HANDLING REQUIREMENTS:

The following requirements must be in place:

A. Background screening of potential Harris Health employees is performed by Human Resources. (See Harris Health Policy 6.12 Employment).

B. Access to Cardholder Data through media such as computers, removable electronic media, paper receipts, paper reports, and faxes are physically secured and restricted to those individuals processing Cardholder Data.

C. Cardholder account numbers on physical forms must be masked to expose at a maximum the first six or the last four digits upon completion of processing such forms.

D. Information Users are prohibited from copying, cutting, pasting, and printing Cardholder Data unless business justification requires the Information User to do so. Information Users should never store or save Cardholder Data onto local hard drives or other external media without express authorization from Information Security.

E. Information Users are prohibited from sending PANs through end-user messaging technologies, such as instant messages, e-mails, or any other social media.

F. Accounts used by vendors to access, support, and maintain system components must be disabled and enabled only when needed by the vendor. Vendor remote access accounts must be monitored when in use.

IV. DISTRIBUTION OF CARDHOLDER DATA MEDIA:

When handling hardcopies and Information Systems that contain Cardholder Data, the following guidelines must be incorporated:

A. The internal and external distribution of cardholder media is strictly permitted to users with a business purpose only.

B. Documented management approval must be obtained for any and all Cardholder Data that is moved from a secure area.

C. In the event that Cardholder Data needs to be physically moved to another location, the Cardholder Data must be transported by a secured courier. Any other method of transportation of Cardholder Data must be approved prior to transportation by Information Security.

D. Inventories of media containing Cardholder Data must be conducted periodically to ensure that Cardholder Data has not been lost in transit or removed without authorization.

V. CARDHOLDER DATA DISPOSAL:

Information Systems or hard copies containing Cardholder Data must be destroyed when the Cardholder Data is no longer needed for business or legal reasons according to the Harris Health Policy 8.03 Records Retention and Destruction. If Information

Users are unsure of which destruction method to use, please contact Harris Health Information Security for further guidance. Appropriate methods of disposal include but are not limited to:

A. Cross-cut shredding of hardcopy materials; and

B. Purging, shredding, or otherwise destroying electronic media so that Cardholder Data cannot be reconstructed via a secure wipe program in accordance with industry-accepted standards for secure deletion, or otherwise physically destroying the media.

VI. ENFORCEMENT:

Workforce member found to have violated this policy may be subject to disciplinary action as outlined in the Harris Health System Policy 3.11.104 Sanctions for Failure to Comply with Health Information Portability and Accountability Act (HIPAA) Privacy and Harris Health Information Security Policies.

REFERENCES/BIBLIOGRAPHY:

Harris Health System Policy and Procedures 3.11.104 Sanctions for Failure to Comply with Health Information Portability and Accountability Act (HIPAA) Privacy and Information Security Policies.

Harris Health System Policy and Procedures 8.03 Records Retention and Destruction.

Harris Health System Policy and Procedures 3.11.905 Payment Care Industry Management.

Harris Health System Policy and Procedures 3.11.903 Payment Care Industry Cardholder System Administrator.

Harris Health System Policy and Procedures 3.11.906 Payment Care Industry Third Party Service Provider.

Harris Health System Policy and Procedures 3.11.904 Payment Care Industry Network Configuration.

Harris Health Policy and Procedures 6.12 Employment.

OFFICE OF PRIMARY RESPONSIBILITY:

Harris Health System Office of Corporate Compliance

REVISION HISTORY:

Effective Date	Version # (If Applicable)	Review/ Revision Date (Indicate Reviewed or Revised)	Approved by:
	1.0	Approved 06/09/2015	Operations Policy Committee
08/28/2015		Approved 08/27/2015	Board of Managers