Carestream Dental ePayment Services

PA-DSS Implementation Guide

Notice

NEITHER CARESTREAM DENTAL NOR ITS PARENTS OR ANY OF ITS SUBSIDIARIES MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, NONINFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

The information in this document is subject to change. Neither Carestream Dental nor its parents or any of its subsidiaries shall be liable for errors contained herein or for incidental damages in conjunction with the furnishing, performance, or use of this material.

Manual Name: Carestream Dental ePayment Services PA-DSS Implementation Guide
Revision Number: 00
Print Date: October 2011

Nothing herein shall be construed as limiting or reducing your obligations to comply with any applicable laws, regulations or industry standards relating to security or otherwise including, but not limited to, PA-DSS and DSS.

About This Guide

To assure that your Carestream installations comply with Payment Application - Data Security Standards (PA-DSS), follow the procedures in this guide. The information in this document is based on PCI Security Standards Council Payment Application Data Security Standards (version 1.2, dated October 2008).

In addition, you should use the practices referenced by the Center for Internet Security (CIS) to enhance system logging, reduce the chance of intrusion, and increase the ability to detect intrusion. To achieve these goals, you should do the following:

- Enable operating system auditing subsystems
- Log individual servers to a centralized logging server
- Disable infrequently-used or frequently vulnerable networking protocols
- Implement certificate-based protocols for access to servers by users and vendors

Note: These standards must be reviewed on a yearly basis, when the application changes, or when the PA-DSS requirements change.

The ePayment application, version 3.1, has been certified to be compliant with PA-DSS, version 1.2.

Related Documentation

See the following documentation for more information:

- Payment Applications Data Security Standard (PA-DSS) at https://www.pcisecuritystandards.org/security_standards/pa_dss.shtml
- Payment Card Industry Data Security Standard (PCI DSS) at https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml
- Open Web Application Security Project (OWASP) at http://www.owasp.org

1 Understanding the ePayment Application

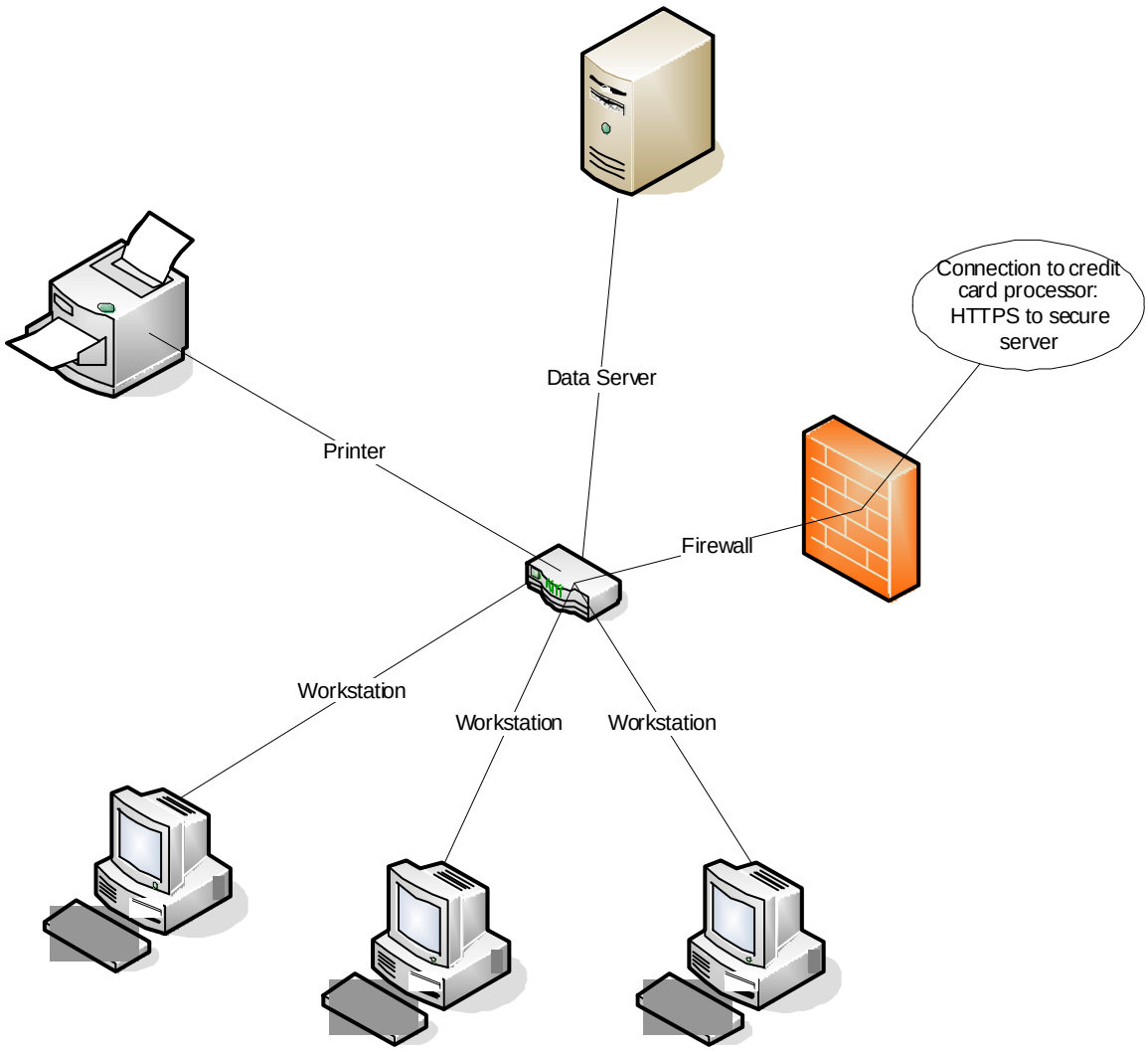
The following list provides information about the ePayment application:

- Name–ePayment Application (pw_iccps.dll)
- Version number–3.1
- Credit card server–TSYS Acquiring Solutions, USA; Global Transport, Canada
- Setup–Carestream Dental implementation specialists assist with all setups.
- Operating systems–Windows VISTA, Windows XP SP3, Windows 2003
- Code base DB engine–Microsoft C++, CTree database
- Description–Integrated payment transaction library for use Carestream Dental practice management software

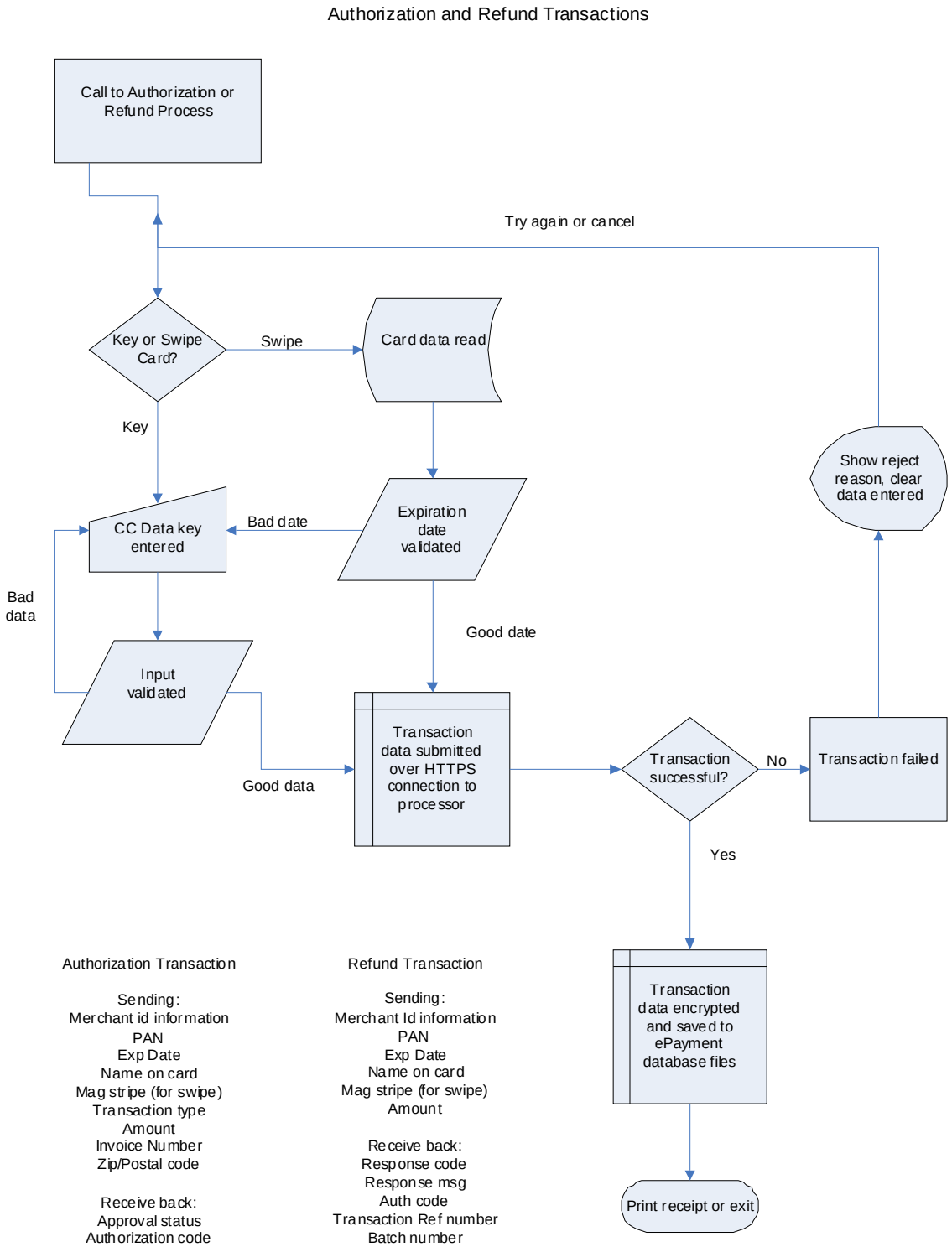
Settlement Dataflow

The settlement process sends a request over a secure Internet connection that all transactions are settled. A response is returned with an accepted or denied status, a count of sales and credits, and the totals for the transactions. All settled transactions display an updated status.

Network Diagram



Dataflow Diagram



2 Understanding PA-DSS Validation and PCI DSS Compliance

The Carestream Dental ePayment application is compliant with Payment Application - Data Security Standards (PA-DSS). The PA-DSS validation ensures that the ePayment application achieves and maintains PCI compliance, when it processes user accounts, passwords, encryption, and other payment data-related information.

The payment card industry (PCI) has developed security standards for handling cardholder information in a published standard called the PCI Data Security Standard (DSS). The security requirements defined in the DSS apply to all members, merchants, and service providers that store, process, or transmit cardholder data.

The PCI DSS requirements apply to all system components within a payment application environment, which is defined as any network device, host, or application included in, or connected to, a network segment where cardholder data is stored, processed, or transmitted.

Obtaining PCI compliance is the responsibility of the customer, using PCI-compliant server architecture with proper hardware and software configurations and access control procedures.

The requirements of the PCI DSS include:

- Install and maintain a firewall configuration to protect data.
- Do not use vendor-supplied defaults for system passwords and other security parameters.
- Protect stored data.
- Encrypt transmission of cardholder data and sensitive information across public networks.
- Use and regularly update anti-virus software.
- Develop and maintain secure systems and applications.
- Restrict access to data by business need-to-know.
- Assign a unique ID to each person with computer access.
- Restrict physical access to cardholder data.
- Track and monitor all access to network resources and cardholder data.
- Regularly test security systems and processes.
- Maintain a policy that addresses information security.

Implementing Payment Applications in a PCI-Compliant Environment

To implement a PCI-compliant environment, perform or observe the following procedures:

- Process sensitive credit card data.
- Remove historical credit card data.
- Set up access controls.
- Properly train and monitor admininstrative personnel.
- Set up management roles and responsibilities.
- Set up PCI-compliant remote access.
- Use SSH, VPN, or SSL/TLS for encryption of administrative access.
- Use compliant log settings.
- Configure PCI-compliant wireless settings.
- Set up data transport encryption.
- Set up PCI-compliant e-mail applications.
- Use network segmentation.
- Never store cardholder data on Internet-accessible systems.
- Use SSL for secure data transmission.
- Deliver PCI-compliant updates.

Processing Sensitive Credit Card Data

To process sensitive credit card data, follow these guidelines:

- Collect sensitive authentication data only when needed to solve a specific problem.
- Store sensitive data only in specific, known locations with limited access.
- Collect only the amount of data needed to solve a specific problem.
- Encrypt sensitive authentication data in storage.
- Securely delete sensitive data immediately after use.

Removing Historical Credit Card Data

Earlier versions of the ePayment application did not store sensitive authentication data; however, encrypted cardholder data is stored and must be purged from the database in the earliest possible timeframe. When transactions are settled, they should be retained only as long as necessary. Your practice management software has a utility that deletes old transactions, as specified by a date that the administrator provides. Depending upon the retention time set by your office, this utility should be run on a regular basis to make sure unnecessary data is not being stored.

Removing Cryptographic Material (PA-DSS, 2.7.a)

To ensure compliance with PCI DSS, cryptographic material must be removed. To securely remove all cryptographic material in versions 2.8 and earlier of the ePayment application, you must install the new ePayment program files and the conversion program for your practice management software. The program runs automatically upon installation, and the encryption of pending transactions is updated.

Note: When you are running version 3.1, view the transactions to re-encrypt historic data with new keys.

Setting Up Access Controls

PCI DSS requires that you use unique user names and strong passwords to access all systems in payment processing. Unique user names indicate that every account is associated with an individual user or process and that no generic group accounts are used.

In addition, you must remove, disable, or rename default accounts provided with operating systems, databases, or devices, if possible. Examples of default administrator accounts are **administrator** (Windows systems), **sa** (SQL/MSDE), and **root** (UNIX/Linux).

Use the following PCI standards for passwords:

- Must be at least 7 characters in length
- Must include both numeric and alphabetic characters
- Must be changed every 90 days
- Must be different from the last 4 passwords

Additional PCI DSS requirements include the following:

- If an incorrect password is provided six times, the account must be locked out.
- The duration of the account lockout must be at least 30 minutes (or until an administrator resets it).
- If a session is idle for more than 15 minutes, the user must re-enter his user name and password to reactivate the session.
- No group, shared, or generic user accounts may be used.

The ePayment application meets or exceeds these requirements. The same standards must be used when setting up network and practice management software user accounts.

Note: These controls apply to employees with administrative capabilities and those who have access to servers with cardholder data.

Training and Monitoring Administrative Personnel

It is your responsibility to train and manage admininstrative users who have access to credit cards, site data, and so forth.

Providing PCI-Compliant Remote Access

The PCI standard requires that if employees, administrators, or vendors are granted remote access to payment processing, access should be authenticated using a two-factor authentication process; for example, a user name/password and an additional authentication item, such as a token or certificate.

In addition to the standard access controls, vendor accounts should be active only while access is required to provide service. Access rights should include only those required for the service rendered and should be audited frequently.

If you use third-party remote access software, such as Remote Desktop (RDP)/Terminal Server, pcAnywhere, and so forth, special standards apply. In addition to the two-factor authentication process, every session must be encrypted with at least 128-bit encryption. For RDP/Terminal Services, use the high encryption setting on the server; for pcAnywhere, use symmetric or public key options for encryption. Additionally, the PCI user account and password requirements apply.

When requesting support from a vendor, reseller, or integrator, take the following precautions:

- Change default settings, such as user names and passwords, on remote access software.
- Allow connections only from specific IP and MAC addresses.
- Use strong passwords for logins.
- Enable encrypted data transmission.
- Enable account lockouts after a certain number of failed login attempts.
- Require that remote access take place over a VPN as opposed to allowing connections directly from the Internet.
- Enable logging for auditing purposes.
- Revoke access as soon as the support task is completed.
- Use SSH, VPN, or SSL/TLS for encryption of administrative access.

Using PCI DSS Log Settings

The ePayment application uses logging by default. This logging cannot be disabled. The following items are logged for all transactions:

- Date
- Time
- User
- Patient
- Amount
- Masked data transmitted
- Success or failure of the transaction

3 To track log files, enable event logging in Windows and audit logging in Windows Explorer.

Important: Before you set up auditing for files and folders, you must enable **Audit Object Access** located in **Audit Policy**. Or you can turn on **Audit Policy** locally for each computer in the **Computer Windows Local Policies**.

To set or view auditing for the log files, run the ePayment application once on each workstation and follow these steps:

1 In Windows Explorer, locate the log file.

2 Right-click on the folder containing the file, click **Properties**, and then click the **Security** tab.

3 Click **Advanced**, and then click the **Auditing** tab.

4 Do the following:

- To set up auditing for all users, click **Add**. In the **Name** field, type **Domain users**, and then select the **Check Names** option. If **Domain users** are underlined, click **OK**.
- In the **Access** section, do the following for each event you want to specify:
  - To audit successful events, select the **Successful** option.
  - To stop auditing successful events, deselect the **Successful** option.
  - To audit unsuccessful events, select the **Failed** option.
  - To stop auditing unsuccessful events, deselect the **Failed** option.
  - To stop auditing all events, click **Clear All**.

5 Make sure the **Inherit from parent the auditing….** option is selected.

Setting Log File Security

In Windows Explorer Security, allow access to the log files only for users with administrative privileges or the appropriate security.

Using PCI-Compliant Wireless Settings

Carestream Dental practice management software and the ePayment application are not supported in a wireless environment. If you install the practice management software in a wireless environment, use compliant wireless settings, per PCI DSS, 1.2.3, 2.1.1, and 4.1.1.

1.2.3

Perimeter firewalls must be installed between any wireless networks and systems that store cardholder data, and these firewalls must deny or control any traffic from the wireless environment into the cardholder data environment.

2.1.1

- All wireless networks must implement strong encryption; for example, AES.
- Encryption keys must be changed from the default at installation and must be changed when an employee with knowledge of the keys leaves the company or changes positions.
- Default SNMP community strings on wireless devices are changed.
- Default passwords and passphrases on access points are changed.
- Firmware on wireless devices is updated to support strong encryption for authentication and transmission over wireless networks; for example, WPA/WPA2.

4.1.1

- Use industry best practices to implement strong encryption for the following over the wireless network in the cardholder data environment:
  - Transmission of cardholder data
  - Transmission of authentication data
- Follow these restrictions regardingthe use of WEP:
  - For new wireless implementations, it is prohibited to use WEP as of March 31, 2009.
  - For current wireless implementations, it is prohibited to use WEP after June 30, 2010.

Using Data Transport Encryption

To safeguard sensitive cardholder data during transmission over public networks, the PCI DSS requires the use of strong cryptography and encryption techniques with at least a 128 bit encryption strength, either at the transport layer with SSL or IPSEC or at the data layer with algorithms, such as RSA or Triple-DES.

See the dataflow diagram for understanding the flow of encrypted data for the ePayment application.

PCI-Compliant Use of User Messaging Technologies

The ePayment application does not send PANs or credit card information by user messaging technology; for example, e-mail, instant messaging, and so forth.

PCI requires that cardholder information is never sent by user messaging technology without strong encryption of the data. The use of a properly installed 128-bit SSL certificate, available from your hosting provider, meets this requirement. The ePayment application can then be configured to transmit securely any page that involves sensitive data, such as login pages, account pages, cart pages, payment pages, and so forth.

Non-Console Administration Access (PA-DSS, 13.1)

The ePayment SDK does not support non-console administrative access.

Using Network Segmentation

The PCI DSS requires that firewall services be used (with NAT or PAT) to break network segments into logical security domains, based on the environmental needs for Internet access. This corresponds to the creation of at least a DMZ and a trusted network segment where only authorized, business-justified traffic from the DMZ is allowed to connect to the trusted segment. No direct incoming Internet traffic to the trusted application environment is allowed. Additionally, outbound Internet access from the trusted segment must be limited to required and justified ports and services.

See the Network diagram for an understanding the flow of encrypted data associated with your practice management software.

Storing Cardholder Data on Internet-Accessible Systems

Never store cardholder data on Internet-accessible systems; for example, the web server and the database server must not be the same server.

Using SSL for Secure Data Transmission

PCI DSS, 4.1, requires that you use strong cryptography and security protocols such as secure sockets layer (SSL) / transport layer security (TLS) and Internet protocol security (IPSEC) to safeguard sensitive cardholder data during transmission over open, public networks.

Examples of open, public networks in the PCI DSS scope are the Internet, WiFi (IEEE 802.11x), global system for mobile communications (GSM), and general packet radio service (GPRS).

PCI DSS, 4.1, requires that for wireless networks transmitting cardholder data, you encrypt the transmissions by using WiFi protected access (WPA or WPA2) technology, IPSEC VPN, or SSL/TLS. Do not rely exclusively on wired equivalent privacy (WEP) to protect confidentiality and access to a wireless LAN.

PCI-Compliant Delivery of Updates

Carestream Dental provides software updates and patches by CD or over the Internet to upgrade your software and to protect you from security threats. The update process validates the existing software prior to installing the new files.

To receive updates and patches by remote access, follow these guidelines:

- Use a personal firewall product if your computer is connected by VPN, or other high-speed connection, to secure all connections, per PCI DSS, 1.3.10.
- Use 2-factor authentication for remote access.
- Use a secure modem, per the following PCI DSS, 12.3:
    - 12.3–Develop usage policies for critical employee-facing technologies (such as modems and wireless) to define proper use of these technologies for all employees and contractors. Ensure these usage policies require the following:
        - 12.3.1–Explicit management approval
        - 12.3.2–Authentication for use of the technology
        - 12.3.3–List of all such devices and personnel with access
        - 12.3.4–Labeling of devices with owner, contact information, and purpose
        - 12.3.5–Acceptable uses of the technologies
        - 12.3.6–Acceptable network locations for the technologies
        - 12.3.7–List of company-approved products
        - 12.3.8–Automatic disconnect of modem sessions after a specific period of inactivity
        - 12.3.9–Activation of modems for vendors only when needed by vendors, with immediate deactivation after use
        - 12.3.10–When accessing cardholder data remotely via modem, prohibition of storage of cardholder data onto local hard drives, floppy disks, or other external media. Prohibition of cut-and-paste and print functions during remote access.

Maintaining an Information Security Program

A comprehensive approach to assessing and maintaining the security compliance of the payment application environment is necessary to protect the organization and sensitive cardholder data.

You should adopt the following plan to develop and implement a security policy and program:

- Read the PCI DSS and perform a security gap analysis. Identify any gaps between existing practices in your organization and those outlined by the PCI requirements.
- Determine the steps you should take to protect cardholder data. Changes could include adding new technologies to aid firewall and perimeter controls, or increasing the logging and archiving procedures associated with transaction data.
- Create an action plan for on-going compliance and assessment.
- Implement, monitor, and maintain the plan. Complete annual self-assessments, using the PCI Self Assessment questionnaire.
- Request assistance from outside experts, as needed.

Configuring the Application System

For PCI DSS compliance, use the following operating systems and dependent application patch levels and configurations supported and tested for continued PCI DSS compliance.

- System Requirements for your practice management software
- Magtek credit card swiper available from Carestream Dental

Initially Setting Up and Configuring the ePayment Application

To set up and configure the application, see the following information:

- The ePayment application is automatically installed with your practice management software.
- The eServices Implementations staff will assist you with creating your merchant account for credit card processing.
- The eServices Implementations staff will walk you through configuring your ePayment application to process credit card transactions, including running test transactions to make sure your system is working correctly.
- The practice owner or office manager should set administrator passwords in your software.
- Perform regular backups as maintenance for your practice. Your network administrator should perform these procedures.