

[PCI DSS v4.0 PDF](#)

Do you ensure inbound traffic permitted to the CDE is restricted to only traffic that is necessary and all other traffic is specifically denied?

- Yes
- No

Only customer can answer this.

Next

[PCI DSS v4.0 PDF](#)

Do you ensure outbound traffic permitted out from the CDE is restricted as follows: To only traffic that is necessary. All other traffic is specifically denied?

- Yes
 - No
- Only customer can answer this.

Previous

Next

[PCI DSS v4.0 PDF](#)

Do you have a wireless network? If so, have network security controls (NSC) been established between the wireless networks and the cardholder data environments? If so, do the NSC's only allow wireless traffic with an authorized business purpose into credit data environments?

- Yes
 - No
- Only customer can answer this.

[PCI DSS v4.0 PDF](#)

Are the processes and mechanisms for applying secure configurations to all system components, including wireless environments:

- Documented?
- Kept up to date?
- In use?
- Known to all affected parties?

Yes
 No

Only customer can answer this.

Previous

Next

[PCI DSS v4.0 PDF](#)

Are configuration standards developed, implemented, and maintained to:

- Cover all system components?
- Address all known security vulnerabilities?
- Be consistent with industry-accepted system hardening standards or vendor hardening recommendations?
- Be updated as new vulnerability issues are identified, as defined in Requirement 6.3.1 (which is stated below)?
- New systems are configured and verified as in place before or immediately after a system component is connected to a production environment?
- 6.3.1 Security vulnerabilities are identified and managed as follows:
 - New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs).
 - Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact.
 - Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment.
 - Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.

Yes
 No

Only customer can answer this.

Previous

Next

[PCI DSS v4.0 PDF](#)

Are vendor default accounts managed as follows: If the vendor default account(s) will be used, the default password is changed per Requirement 8.3.6. If the vendor default account(s) will not be used, the account is removed or disabled?
Refer to page 174 of [PCI DSS v4.0 PDF](#) for Requirement 8.3.6

- Yes
- No

Only customer can answer this.

Previous

Next

[PCI DSS v4.0 PDF](#)

Are primary functions requiring different security levels managed as follows: Only one primary function exists on a system component, OR Primary functions with differing security levels that exist on the same system component are isolated from each other, OR Primary functions with differing security levels on the same system component are all secured to the level required?

- Yes
 - No
- Only customer can answer this.

Previous

Next

[PCI DSS v4.0 PDF](#)

Are only necessary services, protocols, daemons, etc. enabled as required for the function of the system and all unnecessary functionality is removed or disabled?

- Yes
- No

Only customer can answer this.

Previous

Next

[PCI DSS v4.0 PDF](#)

- (A) If any insecure services, protocols, or daemons are present, is business justification documented?
- (B) Are additional security features documented and implemented that reduce the risk of using insecure services, protocols, or daemons?
- (C) Is business justification documented for any present insecure services, protocols, or daemons and are additional security features documented and implemented that reduce the risk of using insecure services, protocols, or daemons?

- Yes
 - No
- Only customer can answer this.

Previous

Next

[PCI DSS v4.0 PDF](#)

Are system security parameters are configured to prevent misuse?

- Yes
- No

Only customer can answer this.

Previous

Next

[PCI DSS v4.0 PDF](#)

Is all non-console administrative access encrypted using strong cryptography.

- Yes
- No

Only customer can answer this.

Previous

Next

[PCI DSS v4.0 PDF](#)

For wireless environments connected to the Card Data Environment(CDE) or transmitting account data, are all wireless vendor defaults changed at installation or are confirmed to be secure, including but not limited to:

- Default wireless encryption keys.
- Passwords on wireless access points.
- SNMP defaults.
- Any other security-related wireless vendor defaults.

Yes Only customer can answer this.
 No

[PCI DSS v4.0 PDF](#)

For wireless environments connected to the CDE or transmitting account data, are wireless encryption keys changed whenever personnel with knowledge of the key leave the the role for which the knowledge was necessary or company; and whenever the key is suspected of or known to be compromised?

- Yes
- No

Only customer can answer this.

Previous

Next

[PCI DSS v4.0 PDF](#)

All security policies and operational procedures that are identified protect stored account data are:

- Documented.
- Kept up to date.
- In use.
- Known to all affected parties.

Yes
 No

Only customer can answer this.

Previous

Next

[PCI DSS v4.0 PDF](#)

Do you ensure SAD is not retained after authorization, even if encrypted and all sensitive authentication data received is rendered unrecoverable upon completion of the authorization process?

- Yes
- No

ChiroSpring Pay stores a secure token only (which means the card can only be used in ChiroSpring and not anywhere else). No card data is stored on our servers or the customer's computer. This includes card number, expiration date and security code.

Previous

Next

[PCI DSS v4.0 PDF](#)

Do you ensure the card verification code is not retained upon completion of the authorization process?

- Yes
- No

ChiroSpring Pay stores a secure token only (which means the card can only be used in ChiroSpring and not anywhere else). No card data is stored on our servers or the customer's computer. This includes card number, expiration date and security code.

Previous

Next

[PCI DSS v4.0 PDF](#)

Is cardholder account data (PAN) masked when displayed such that only personnel with a legitimate business need can see more than the BIN (the first six or eight digits) and last four digits of the PAN?

- Yes
- No

Yes. After a card is entered into ChiroSpring only the last four digits are visible.

Previous

Next

[PCI DSS v4.0 PDF](#)

Are strong cryptography and security protocols such as HTTPS or SSH used to safeguard sensitive cardholder data (PAN) during transmission over open, public networks, and are the following requirements implemented?

- Only trusted keys and certificates are accepted.
- Certificates used to safeguard PAN during transmission over open, public networks are confirmed as valid and are not expired or revoked.
- The protocol in use supports only secure versions or configurations and does not support fallback to, or use of insecure versions, algorithms, key sizes, or implementations.
- The encryption strength is appropriate for the encryption methodology in use.

Further Information

Vendor recommendations and industry best practices can be consulted for information about the proper encryption strength specific to the encryption methodology in use.

For more information about strong cryptography and secure protocols, see industry standards and best practices such as NIST SP 800-52 and SP 800-57.

For more information about trusted keys and certificates, see NIST Cybersecurity Practice Guide Special Publication 1800-16, Securing Web Transactions: Transport Layer Security (TLS) Server Certificate Management.

- Yes
 No

Yes. ChiroSpring Pay supports all of these measures.

[PCI DSS v4.0 PDF](#)

Do you ensure that wireless networks transmitting PAN or connected to the card data environment (CDE) uses industry best practices to implement strong cryptography for authentication and transmission?

- Yes
- No

Only customer can answer this.

[PCI DSS v4.0 PDF](#)

Is antivirus software installed on all servers and workstations, and is it configured as follows?

- Automatically install updates
- Generate audit logs
- Remove other forms of malicious software including spyware and adware
- Periodic scans enabled
- Network only - master installation enabled for automatic updates and scans

- Yes
- No

For this question, it sounds like they are referencing the customer's internal computer network. Of note, ChiroSpring ensures all of its servers are updated, using antivirus and secure.

[PCI DSS v4.0 PDF](#)

Has an anti-malware solution(s) been deployed on all system components except for those identified in periodic evaluations that concludes the system components are not at risk from malware (Requirement 5.2.3)?
Refer to page 115 of [PCI DSS v4.0 PDF](#) for Req 5.2.3

- Yes
 - No
- For this question, it sounds like they are referencing the customer's internal computer network. Of note, ChiroSpring ensures all of its servers are updated, using antivirus and secure.

[PCI DSS v4.0 PDF](#)

Does the deployed anti-malware solution(s) detect all types of malware and removes, blocks or contains all known types of malware?

- Yes
 - No
- For this question, it sounds like they are referencing the customer's internal computer network. Of note, ChiroSpring ensures all of its servers are updated, using antivirus and secure.

Previous

Next

[PCI DSS v4.0 PDF](#)

Are system components not at risk for malware periodically evaluated and do those evaluations include the following?

- A documented list of all system components not at risk for malware.
- Identification and evaluation of evolving malware threats for those system components.
- Confirmation whether such system components continue to not require anti-malware protection.

Yes

No

Only customer can answer this.

Previous

[PCI DSS v4.0 PDF](#)

Is the frequency of periodic evaluations of system components identified as not at risk for malware defined for your organization in a targeted risk analysis which was performed according to the following elements?

- Identification of the assets being protected.
- Identification of the threat(s) that the requirement is protecting against.
- Identification of factors that contribute to the likelihood and/or impact of a threat being realized.
- Resulting analysis that determines, and includes justification for, how frequently the requirement must be performed to minimize the likelihood of the threat being realized.
- Review of each targeted risk analysis at least once every 12 months to determine whether the results are still valid or if an updated risk analysis is needed.
- Performance of updated risk analyses when needed, as determined by the annual review.

Yes

No

Only customer can answer this.

Previous

[PCI DSS v4.0 PDF](#)

Is your Anti-malware solution kept current via automatic updates?

- Yes
 - No
- Only customer can answer this.

Previous

Next

[PCI DSS v4.0 PDF](#)

Does your anti-malware solution perform periodic scans and active or real-time scans OR perform continuous behavioral analysis of systems or processes?

- Yes
 - No
- Only customer can answer this.

Previous

Next

[PCI DSS v4.0 PDF](#)

Are periodic malware scans performed? If so, do the scans happen at a frequency defined in a targeted risk analysis (TRA).

Note: The TRA must include the following:

- Identification of the assets being protected.
- Identification of the threat(s) that the requirement is protecting against.
- Identification of factors that contribute to the likelihood and/or impact of a threat being realized.
- Resulting analysis that determines, and includes justification for, how frequently the requirement must be performed to minimize the likelihood of the threat being realized.
- Review of each targeted risk analysis at least once every 12 months to determine whether the results are still valid or if an updated risk analysis is needed.
- Performance of updated risk analyses when needed, as determined by the annual review.

- Yes
- No

Only customer can answer this.

Previous

Next

[PCI DSS v4.0 PDF](#)

Does the antimalware solution your organization uses perform one of the following on removable electronic media?

Automatic scans when the media is inserted, connected, or logically mounted?

OR

Continuous behavioral analysis of systems or processes when the media is inserted, connected, or logically mounted?

Yes

No

Only customer can answer this.

Previous

Next

[PCI DSS v4.0 PDF](#)

Are audit logs for the anti-malware solution(s) enabled and is the log history retained for at least 12 months, with at least the most recent three months immediately available for analysis.?

- Yes
 - No
- Only customer can answer this.

Previous

Next

[PCI DSS v4.0 PDF](#)

Have you ensured Anti-malware mechanisms cannot be disabled or altered by users, unless specifically documented, and authorized by management on a case-by-case basis for a limited time period?

- Yes
- No

Only customer can answer this.

[PCI DSS v4.0 PDF](#)

Are processes and automated mechanisms in place to detect and protect personnel against phishing attacks?

- Yes
 - No
- Only customer can answer this.

Previous

Next

[PCI DSS v4.0 PDF](#)

Are bespoke and custom software developed securely, as follows:

- Based on industry standards and/or best practices for secure development?
- In accordance with [PCI DSS](#) (for example, secure authentication and [logging](#))?
- Incorporating consideration of [information security](#) issues during each stage of the [software development lifecycle](#)?

- Yes
- No

ChiroSpring and ChiroSpring Pay meet all of these standards. If you are using any other custom software made specifically for your practice you will need to meet the above requirements.

Previous

Next

[PCI DSS v4.0 PDF](#)

Are bespoke and custom software developed securely, as follows:

- Based on industry standards and/or best practices for secure development?

- Yes
- No

ChiroSpring and ChiroSpring Pay meet all of these standards. If you are using any other custom software made specifically for your practice you will need to meet the above requirements.

[PCI DSS v4.0 PDF](#)

If manual code reviews are performed for bespoke and custom software prior to release to production, do you ensure the code changes are:

- Reviewed by individuals other than the originating code author, and who are knowledgeable about code-review techniques and secure coding practices?
- Reviewed and approved by management prior to release?

Yes **ChiroSpring and ChiroSpring Pay meet all of these standards. If you are using any other custom software made specifically for your practice you will need to meet the above requirements.**

No

[PCI DSS v4.0 PDF](#)

ChiroSpring and ChiroSpring Pay meet all of these standards. If you are using any other custom software made specifically for your practice you will need to meet the above requirements.

Are software engineering techniques or other methods defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in bespoke and custom software, including but not limited to the following:

- Injection attacks, including SQL, LDAP, XPath, or other command, parameter, object, fault, or injection-type flaws?
- Attacks on data and data structures, including attempts to manipulate buffers, pointers, input data, or shared data?
- Attacks on cryptography usage, including attempts to exploit weak, insecure, or inappropriate cryptographic implementations, algorithms, cipher suites, or modes of operation?
- Attacks on business logic, including attempts to abuse or bypass application features and functionalities through the manipulation of APIs, communication protocols and channels, client side functionality, or other system/application functions and resources. This includes cross-site scripting (XSS) and cross-site request forgery (CSRF)?
- Attacks on access control mechanisms, including attempts to bypass or abuse identification, authentication, or authorization mechanisms, or attempts to exploit weaknesses in the implementation of such mechanisms?
- Attacks via any “high-risk” vulnerabilities identified in the vulnerability identification process, as defined in Requirement 6.3.1 listed below?
- New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs).
- Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact.
- Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment.
- Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.

[PCI DSS v4.0 PDF](#)

Are security vulnerabilities identified and managed as follows?

- New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs).
- Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact.
- Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment.
- Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.

- Yes **ChiroSpring and ChiroSpring Pay meet all of these standards. For your own internal network and software applications we cannot answer for you.**
- No

[PCI DSS v4.0 PDF](#)

Are security vulnerabilities identified and managed as follows?

- New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs).
- Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact.
- Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment.
- Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.

- Yes **ChiroSpring and ChiroSpring Pay meet all of these standards. For your own internal network and software applications we cannot answer for you.**
- No

[PCI DSS v4.0 PDF](#)

Are all system components protected from known vulnerabilities by installing applicable security patches/updates as follows:

- Critical or high-security patches/updates (identified according to the risk ranking process at Requirement 6.3.1 which is listed below) are installed within one month of release?
- All other applicable security patches/updates are installed within an appropriate time frame as determined by the entity (for example, within three months of release)?
- New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs).
- Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact.
- Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment.
- Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.

- Yes **ChiroSpring and ChiroSpring Pay meet all of these standards. For your own internal network and software applications we cannot answer for you.**
- No

[PCI DSS v4.0 PDF](#)

Are all system components protected from known vulnerabilities by installing applicable security patches/updates as follows:

- Critical or high-security patches/updates (identified according to the risk ranking process at Requirement 6.3.1 which is listed below) are installed within one month of release?
- New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs).
- Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact.
- Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment.
- Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.

- Yes **ChiroSpring and ChiroSpring Pay meet all of these standards. For your own internal network and software applications we cannot answer for you.**
- No

[PCI DSS v4.0 PDF](#)

Are applications developed based on secure coding guidelines in order to protect applications from, at a minimum, the following vulnerabilities? Note: The vulnerabilities listed below were current with industry best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the Open Web Application Security Project (OWASP) Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements

- Do coding techniques address injection flaws, particularly SQL injection? Note: Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.
- Do coding techniques address buffer overflow vulnerabilities?
- Do coding techniques address insecure cryptographic storage?
- Do coding techniques address insecure communications?
- Do coding techniques address improper error handling?
- Do coding techniques address all “high risk” vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1)?

Yes **ChiroSpring and ChiroSpring Pay meet all of these standards. For your own internal network and software applications we cannot answer for you.**

No

[PCI DSS v4.0 PDF](#)

Is access assigned to users, including privileged users, based on:

- Job classification and function?
- Least privileges necessary to perform job responsibilities?

Yes

No **Only customer can answer this.**

Previous

[PCI DSS v4.0 PDF](#)

Are required privileges approved by authorized personnel?

- Yes
 - No
- Only customer can answer this.

Previous

[PCI DSS v4.0 PDF](#)

Are all user accounts and related access privileges, including third-party/vendor accounts, on in-scope system components reviewed as follows?

- At least once every six months.
- To ensure user accounts and access remain appropriate based on job function.
- Any inappropriate access is addressed.
- Management acknowledges that access remains appropriate.

Yes **Only customer can answer this.**
 No

[PCI DSS v4.0 PDF](#)

Are all application and system accounts and related access privileges assigned and managed as follows:

- Based on the least privileges necessary for the operability of the system or application?
- Access is limited to the systems, applications, or processes that specifically require their use?

- Yes
- No

Only customer can answer this.

[PCI DSS v4.0 PDF](#)

Have you ensured practices to identify users and authenticate access to system components are:

- Documented?
- Kept up to date?
- In use?
- Known to all affected parties?

Yes **Only customer can answer this.**
 No

[PCI DSS v4.0 PDF](#)

Are all users assigned a unique ID before access to system components or cardholder data is allowed?

- Yes
 - No
- Only customer can answer this. For ChiroSpring you should ensure all of your staff have their own username and password.

[PCI DSS v4.0 PDF](#)

Are group, shared, or generic accounts, or other shared authentication credentials only used when necessary on an exception basis, and managed as follows?

- Account use is prevented unless needed for an exceptional circumstance.
- Use is limited to the time needed for the exceptional circumstance.
- Business justification for use is documented.
- Use is explicitly approved by management.
- Individual user identity is confirmed before access to an account is granted.
- Every action taken is attributable to an individual user.

Yes

No

Only customer can answer this.

Previous

[PCI DSS v4.0 PDF](#)

Have you ensured addition, deletion, and modification of user IDs, authentication factors, and other identifier objects are managed as follows?

- Authorized with the appropriate approval.
- Implemented with only the privileges specified on the documented approval.

Yes

No

Only customer can answer this.

[PCI DSS v4.0 PDF](#)

Is access for terminated users immediately revoked by adhering to the following procedures?

- You examine information sources for terminated users and review current user access lists—for both local and remote access—to verify that terminated user IDs have been deactivated or removed from the access lists.
- You interview responsible personnel to verify that all physical authentication factors—such as, smart cards, tokens, etc.—have been returned or deactivated for terminated users.

- Yes Only customer can answer this. If a staff member is terminated you must mark them inactive in ChiroSpring.
- No

[PCI DSS v4.0 PDF](#)

Do you ensure Inactive user accounts are removed or disabled within 90 days of inactivity?

- Yes
- No

Only customer can answer this.

Previous

Next

[PCI DSS v4.0 PDF](#)

Are accounts used by third parties to access, support, or maintain system components via remote access managed as follows?

- These accounts are enabled only during the time period needed and disabled when not in use.
- Use is monitored for unexpected activity.

- Yes
- No

Only customer can answer this.

[PCI DSS v4.0 PDF](#)

If a user session has been idle for more than 15 minutes, do you require the user to re-authenticate to re-activate the terminal or session?

- Yes
 - No
- Only customer can answer this.

Previous

[PCI DSS v4.0 PDF](#)

Are all user access to system components for users and administrators authenticated via at least one of the following authentication factors:

- Something you know, such as a password or passphrase?
- Something you have, such as a token device or smart card?
- Something you are, such as a biometric element?

Refer to page 171 of PCI DSS v4.0 PDF for Requirement 8.3.1

- Yes
 - No
- Only customer can answer this.

[PCI DSS v4.0 PDF](#)

Do you allow anyone to access your credit card information remotely from outside your facility using telephone modems, remote access software such as PC Anywhere or a virtual private network (VPN)?

Yes

No

Only customer can answer this.

Previous

[PCI DSS v4.0 PDF](#)

Is a user identity verified before modifying any authentication factor.

- Yes **Only customer can answer this.**
- No

[PCI DSS v4.0 PDF](#)

For the authentication service(s) used to provide access to in-scope system components, are invalid authentication attempts limited by:

- Locking out the user ID after not more than 10 attempts?
- Setting the lockout duration to a minimum of 30 minutes or until the user's identity is confirmed?

Yes

No

You can set these on your Mac or PC.

[PCI DSS v4.0 PDF](#)

If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, are they set and reset for each user as follows:

- Set to a unique value for first-time use and upon reset?
- Forced to be changed immediately after the first use?

Refer to page 171 of PCI DSS v4.0 PDF for Requirement 8.3.1

- Yes
- No

Only customer can answer this.

[PCI DSS v4.0 PDF](#)

If passwords/passphrases are used as authentication factors to provide access to in-scope system components, are they required to meet the following minimum level of complexity?

- A minimum length of 12 characters (or IF the system does not support 12 characters, a minimum length of eight characters).
- Contain both numeric and alphabetic characters.

Yes

No

Only customer can answer this.

[PCI DSS v4.0 PDF](#)

Do you ensure Individuals are not allowed to submit a new password/passphrase that is the same as any of the last four passwords/passphrases used?

- Yes
 - No
- Only customer can answer this.

Previous

[PCI DSS v4.0 PDF](#)

Do you ensure a authentication policies and procedures are documented and communicated to all users including the following?

- Guidance on selecting strong authentication factors.
- Guidance for how users should protect their authentication factors.
- Instructions not to reuse previously used passwords/passphrases.
- Instructions to change passwords/passphrases if there is any suspicion or knowledge that the password/passphrases have been compromised and how to report the incident.

Yes
 No **Only customer can answer this.**

[PCI DSS v4.0 PDF](#)

If passwords/passphrases are used as the only authentication factor for user access (i.e., in any single-factor authentication implementation), are the passwords/passphrases changed at least once every 90 days OR the security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly?

- Yes
 - No
- Only customer can answer this.

[PCI DSS v4.0 PDF](#)

Is MFA implemented for all non-console access into the CDE for personnel with administrative access?

- Yes
 - No
- Only customer can answer this.

Previous

[PCI DSS v4.0 PDF](#)

Is MFA implemented for all access into the card data environments(CDE)?

- Yes
 - No
- Card data is not stored in ChiroSpring (only a secure token is stored). ChiroSpring does not support MFA. Since there are no card data environments, you can probably say 'Yes' here.

Previous

[PCI DSS v4.0 PDF](#)

Do you ensure MFA is implemented for all remote network access originating from outside the entity's network that could access or impact the CDE as follows?

- All remote access by all personnel, both users and administrators, originating from outside the entity's network.
- All remote access by third parties and vendors.

- Yes
- No

Only customer can answer this.

[PCI DSS v4.0 PDF](#)

Are MFA systems in use to support authentication to or within the CDE implemented as follows:

- The MFA system is not susceptible to replay attacks?
- MFA systems cannot be bypassed by any users, including administrative users unless specifically documented, and authorized by management on an exception basis, for a limited time period?
- At least two different types of authentication factors are used.
- Success of all authentication factors is required before access is granted?

Yes **Only customer can answer this.**
 No

[PCI DSS v4.0 PDF](#)

For the authentication service(s) used to provide access to in-scope system components, can accounts used by systems or applications be used for interactive login (meaning a human could use the credentials to login)? If so, are they managed as follows?

- Interactive use is prevented unless needed for an exceptional circumstance.
- Interactive use is limited to the time needed for the exceptional circumstance.
- Business justification for interactive use is documented.
- Interactive use is explicitly approved by management.
- Individual user identity is confirmed before access to account is granted.
- Every action taken is attributable to an individual user.

Yes **Only customer can answer this.**
 No

[PCI DSS v4.0 PDF](#)

Are passwords/passphrases for any application and system accounts that can be used for interactive login (meaning a human could use the credentials to login) hard coded in scripts, configuration/property files, or bespoke and custom source code?

- Yes
 - No
- Only customer can answer this. The answer is 'No' for the ChiroSpring application.

[PCI DSS v4.0 PDF](#)

Are Passwords/passphrases for any application and system accounts protected against misuse as follows:

- Passwords/passphrases are changed periodically (at the frequency defined in the entity's targeted risk analysis (TRA)) and upon suspicion or confirmation of compromise? Note: The TRA must include the following:
 - Identification of the assets being protected.
 - Identification of the threat(s) that the requirement is protecting against.
 - Identification of factors that contribute to the likelihood and/or impact of a threat being realized.
 - Resulting analysis that determines, and includes justification for, how frequently the requirement must be performed to minimize the likelihood of the threat being realized.
 - Review of each targeted risk analysis at least once every 12 months to determine whether the results are still valid or if an updated risk analysis is needed.
 - Performance of updated risk analyses when needed, as determined by the annual review.
- Passwords/passphrases are constructed with sufficient complexity appropriate for how frequently the entity changes the passwords/passphrases?

Yes

No

Only customer can answer this.

Previous

[PCI DSS v4.0 PDF](#)

Any physical access to cardholder data or systems that store, process, or transmit cardholder data provides the opportunity for individuals to access and/or remove systems or hardcopies containing cardholder data; therefore have you ensured your policies and procedures for restriction of physical access are:

- Documented?
- Kept up to date?
- In use?
- Known to all affected parties?

- Yes
- No

ChiroSpring Pay does not store card data on your computer or on our servers. We only store a secure token. You can probably answer 'Yes'. Just make sure you have a policy that ensures no one is writing down card holder data in any system outside of ChiroSpring and that the data entry in ChiroSpring is only in the appropriate ChiroSpring Pay payment box (not in any other note box, etc.).

[PCI DSS v4.0 PDF](#)

Are appropriate facility entry controls in place to restrict physical access to systems in the card data environment (CDE)?

- Yes
 - No
- ChiroSpring Pay does not store card data on your computer or on our servers. We only store a secure token. You can probably answer 'Yes'. Just make sure you have a policy that ensures no one is writing down card holder data in any system outside of ChiroSpring and that the data entry in ChiroSpring is only in the appropriate ChiroSpring Pay payment box (not in any other note box, etc.).

[PCI DSS v4.0 PDF](#)

Is individual physical access to sensitive areas within the card data environment(CDE) monitored with either video cameras or physical access control mechanisms (or both) as follows?

- Entry and exit points to/from sensitive areas within the CDE are monitored.
- Monitoring devices or mechanisms are protected from tampering or disabling.
- Collected data is reviewed and correlated with other entries.
- Collected data is stored for at least three months, unless otherwise restricted by law.

- Yes **ChiroSpring Pay does not store card data on your computer or on our servers.**
- No **We only store a secure token. You can probably answer 'Yes'. Just make sure you have a policy that ensures no one is writing down card holder data in any system outside of ChiroSpring and that the data entry in ChiroSpring is only in the appropriate ChiroSpring Pay payment box (not in any other note box, etc.).**

[PCI DSS v4.0 PDF](#)

Are physical and/or logical controls implemented to restrict use of publicly accessible network jacks within the facility?

- Yes
 - No
- ChiroSpring Pay does not store card data on your computer or on our servers. We only store a secure token. You can probably answer 'Yes'. Just make sure you have a policy that ensures no one is writing down card holder data in any system outside of ChiroSpring and that the data entry in ChiroSpring is only in the appropriate ChiroSpring Pay payment box (not in any other note box, etc.).

[PCI DSS v4.0 PDF](#)

Is all media with cardholder data is physically secured?

- Yes ChiroSpring Pay does not store card data on your computer or on our servers.
- No We only store a secure token. You can probably answer 'Yes'. Just make sure you have a policy that ensures no one is writing down card holder data in any system outside of ChiroSpring and that the data entry in ChiroSpring is only in the appropriate ChiroSpring Pay payment box (not in any other note box, etc.).

[PCI DSS v4.0 PDF](#)

Are offline media backups with cardholder data are stored in a secure location?

- Yes ChiroSpring Pay does not store card data on your computer or on our servers.
- No We only store a secure token. You can probably answer 'Yes'. Just make sure you have a policy that ensures no one is writing down card holder data in any system outside of ChiroSpring and that the data entry in ChiroSpring is only in the appropriate ChiroSpring Pay payment box (not in any other note box, etc.).

[PCI DSS v4.0 PDF](#)

Is all media with cardholder data classified in accordance with the sensitivity of the data?

- Yes **ChiroSpring Pay does not store card data on your computer or on our servers.**
- No **We only store a secure token. You can probably answer 'Yes'. Just make sure you have a policy that ensures no one is writing down card holder data in any system outside of ChiroSpring and that the data entry in ChiroSpring is only in the appropriate ChiroSpring Pay payment box (not in any other note box, etc.).**

[PCI DSS v4.0 PDF](#)

Is media with cardholder data sent outside the facility secured as follows?

- Media sent outside the facility is logged.
- Media is sent by secured courier or other delivery method that can be accurately tracked.
- Offsite tracking logs include details about media location.

- Yes ChiroSpring Pay does not store card data on your computer or on our servers.
- No We only store a secure token. You can probably answer 'Yes'. Just make sure you have a policy that ensures no one is writing down card holder data in any system outside of ChiroSpring and that the data entry in ChiroSpring is only in the appropriate ChiroSpring Pay payment box (not in any other note box, etc.).

[PCI DSS v4.0 PDF](#)

Is media with cardholder data sent outside the facility secured as follows?

- Media is sent by secured courier or other delivery method that can be accurately tracked.

- Yes** ChiroSpring Pay does not store card data on your computer or on our servers.
- No** We only store a secure token. You can probably answer 'Yes'. Just make sure you have a policy that ensures no one is writing down card holder data in any system outside of ChiroSpring and that the data entry in ChiroSpring is only in the appropriate ChiroSpring Pay payment box (not in any other note box, etc.).

[PCI DSS v4.0 PDF](#)

Are hard-copy materials with cardholder data destroyed when no longer needed for business or legal reasons, as follows:

- Are materials cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed?
- Are materials stored in secure storage containers prior to destruction?

- Yes** ChiroSpring Pay does not store card data on your computer or on our servers.
- No** We only store a secure token. You can probably answer 'Yes'. Just make sure you have a policy that ensures no one is writing down card holder data in any system outside of ChiroSpring and that the data entry in ChiroSpring is only in the appropriate ChiroSpring Pay payment box (not in any other note box, etc.).

[PCI DSS v4.0 PDF](#)

Are POI devices that capture payment card data via direct physical interaction with the payment card form factor protected from tampering and unauthorized substitution, including the following:

- Maintaining a list of POI devices?
- Periodically inspecting POI devices to look for tampering or unauthorized substitution?
- Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices?

- Yes
- No

Only customer can answer this.

[PCI DSS v4.0 PDF](#)

Do you have an up-to-date list of POI devices maintained to include the following?

- Make and model of the device.
- Location of device.
- Device serial number or other methods of unique identification.

- Yes
- No

Only customer can answer this.

Previous

[PCI DSS v4.0 PDF](#)

Are POI device surfaces periodically inspected to detect tampering and unauthorized substitution?

- Yes
 - No
- Only customer can answer this.

Previous

[PCI DSS v4.0 PDF](#)

Is training provided for personnel in POI environments to be aware of attempted tampering or replacement of POI devices, and includes the following?

- Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, before granting them access to modify or troubleshoot devices.
- Procedures to ensure devices are not installed, replaced, or returned without verification.
- Being aware of suspicious behavior around devices.
- Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel.

- Yes
- No

Only customer can answer this.

[PCI DSS v4.0 PDF](#)

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs on all system components and in the cardholder data environment (CDE) allows thorough tracking, alerting, and analysis when something does go wrong. Are policies and procedures for logging and monitoring all access to system components and cardholder data:

- Documented?
- Kept up to date?
- In use?
- Known to all affected parties?

- Yes
- No

ChiroSpring provides user logs.

[PCI DSS v4.0 PDF](#)

Do you ensure audit logs capture all actions taken by any individual with administrative access, including any interactive use of application or system accounts?

- Yes
- No **ChiroSpring provides user logs.**

[PCI DSS v4.0 PDF](#)

Do your audit logs capture all invalid logical access attempts?

- Yes **ChiroSpring provides user logs including invalid login attempts.**
- No

Previous

[PCI DSS v4.0 PDF](#)

Do your audit logs capture all changes to identification and authentication credentials including, but not limited the following?

- Creation of new accounts.
- Elevation of privileges.
- All changes, additions, or deletions to accounts with administrative access.

- Yes **ChiroSpring provides user audit logs. For information not found in our audit logs we can query the database for this information.**
- No

[PCI DSS v4.0 PDF](#)

Do your audit logs record the following details for each auditable event?

- User identification.
- Type of event.
- Date and time.
- Success and failure indication.
- Origination of event.
- Identity or name of affected data, system component, resource, or service (for example, name and protocol).

- Yes **ChiroSpring provides user audit logs. For information not found in our audit logs we can query the database for this information.**
- No

Previous

Next

[PCI DSS v4.0 PDF](#)

Is read access to audit logs files is limited to those with a job-related need.

- Yes **Only Admin and Provider roles, in ChiroSpring, can access audit logs.**
- No

Previous

Next

[PCI DSS v4.0 PDF](#)

Are Audit log files protected to prevent modifications by individuals?

- Yes
 - No
- Audit logs, in ChiroSpring, cannot be modified by users.

Previous

Next

[PCI DSS v4.0 PDF](#)

Are Audit log files, including those for external-facing technologies, promptly backed up to a secure, central, internal log server(s) or other media that is difficult to modify?

- Yes
- No **Audit logs, in ChiroSpring, cannot be modified by users.**

[PCI DSS v4.0 PDF](#)

Is file integrity monitoring or change-detection mechanisms used on audit logs to ensure that existing log data cannot be changed without generating alerts?

- Yes
 - No
- Audit logs, in ChiroSpring, cannot be modified by users.

[PCI DSS v4.0 PDF](#)

Are the following audit logs reviewed at least once a day?:

- All security events.
- Logs of all system components that store, process, or transmit CHD and/or SAD.
- Logs of all critical system components.
- Logs of all servers and system components that perform security functions (for example, network security controls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers).

Yes **Only customer can answer this.**
 No

Previous

Next

[PCI DSS v4.0 PDF](#)

Are automated mechanisms (e.g. SIEM monitoring) used to perform log reviews?

- Yes **Only customer can answer this.**
- No

Previous

[PCI DSS v4.0 PDF](#)

Do you examine security policies and procedures to verify that processes are defined for reviewing logs of all other system components periodically and examine documented results of log reviews and interview personnel to verify that log Customized Approach Objective reviews are performed periodically?

- Yes
- No Only customer can answer this.

[PCI DSS v4.0 PDF](#)

Do you perform log reviews for lower-risk system components at a frequency that is defined in a targeted risk analysis according to all the following elements?

- Identification of the assets being protected.
- Identification of the threat(s) that the requirement is protecting against.
- Identification of factors that contribute to the likelihood and/or impact of a threat being realized.
- Resulting analysis that determines, and includes justification for, how frequently the requirement must be performed to minimize the likelihood of the threat being realized.
- Review of each targeted risk analysis at least once every 12 months to determine whether the results are still valid or if an updated risk analysis is needed.
- Performance of updated risk analyses when needed, as determined by the annual review.

- Yes
- No **Only customer can answer this.**

[PCI DSS v4.0 PDF](#)

Do you examined security policies and procedures to verify that processes are defined for addressing exceptions and anomalies identified during the review process and observe processes and interview personnel to verify that, when exceptions and Customized Approach Objective anomalies are identified, they are addressed?

- Yes
 - No
- Only customer can answer this.

Previous

Next

[PCI DSS v4.0 PDF](#)

Are audit log retention policies and procedures in place and do they require that logs are retained for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup)?

- Yes Only customer can answer this. The customer should export
- No logs on a monthly basis if they wish to retain them.

[PCI DSS v4.0 PDF](#)

Are all critical system clocks and times synchronized through use of time synchronization technology, and is that technology kept current through managing vulnerabilities and patching the technology according to PCI DSS Requirements 6.3.1 and 6.3.3?

Note: One example of time synchronization technology is Network Time Protocol (NTP).

Refer to pages 133-135, 17 of PCI DSS v4.0 PDF for Requirements 6.3.1 and 6.3.3

- Yes **ChiroSpring ensures all server**
- No **clocks are synchronized.**

[PCI DSS v4.0 PDF](#)

Do one or more designated servers receive time signals from external sources, and do all critical systems have the correct and consistent time, based on International Atomic Time or UTC, and do designated central time servers peer with each other to keep accurate time, and do the designated time server(s) accept time updates only from specific industry-accepted external sources, and do other internal servers only receive time from the central time servers?

- Yes ChiroSpring ensures all server clocks are synchronized.
- No

Previous

Next

[PCI DSS v4.0 PDF](#)

Have you examined system configurations and time-synchronization settings to verify that access to time data is restricted to only personnel with a business need and have you verified that any changes to the time settings, logs and observed processes on critical systems are logged, monitored, and reviewed?

- Yes **ChiroSpring ensures all server**
- No **clocks are synchronized.**

Previous

Next

[PCI DSS v4.0 PDF](#)

Are authorized and unauthorized wireless access points are managed as follows?

- The presence of wireless (Wi-Fi) access points is tested for.
- All authorized and unauthorized wireless access points are detected and identified.
- Testing, detection, and identification occurs at least once every three months.
- If automated monitoring is used, personnel are notified via generated alerts.

Yes **Only customer can answer this.**
 No

[PCI DSS v4.0 PDF](#)

Do you have an inventory of authorized wireless access points maintained, including a documented business justification?

- Yes
- No **Only customer can answer this.**

Previous

[PCI DSS v4.0 PDF](#)

Are internal vulnerability scans performed as follows?

- At least once every three months.
- High-risk and critical vulnerabilities (per the entity's vulnerability risk rankings defined at Requirement 6.3.1) are resolved.
- Rescans are performed that confirm all high-risk and critical vulnerabilities (as noted above) have been resolved.
- Scan tool is kept up to date with latest vulnerability information.
- Scans are performed by qualified personnel and organizational independence of the tester exists.

Refer to page 133 of PCI DSS v4.0 PDF for Requirement 6.3.1

- Yes **ChiroSpring performs quarterly vulnerability scans. Internal scans would need to be**
- No **performed by the customer if needed.**

[PCI DSS v4.0 PDF](#)

Are Internal vulnerability scans performed after any significant change as follows?

- High-risk and critical vulnerabilities (per the entity's vulnerability risk rankings defined at Requirement 6.3.1) are resolved.
- Rescans are conducted as needed.
- Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV).

- Yes **ChiroSpring performs quarterly vulnerability scans. Internal scans would need to be performed by the customer if needed.**
- No

[PCI DSS v4.0 PDF](#)

Are you performing vulnerability scans:

- At least once every three months?
- By a PCI SSC Approved Scanning Vendor (ASV)?
- Vulnerabilities are resolved and ASV Program Guide requirements for a passing scan are met?
- And rescans are performed as needed to confirm that vulnerabilities are resolved per the ASV Program Guide requirements for passing scan?

- Yes **ChiroSpring performs quarterly vulnerability scans. Internal scans would need to be performed by the customer if needed.**
- No

[PCI DSS v4.0 PDF](#)

When performing external vulnerability scans after a significant change, are the vulnerabilities that are scored 4.0 or higher by CVSS are resolved, rescans conducted as needed, and scans performed by qualified personnel and organizational independence of the tester exists?

- Yes **ChiroSpring performs quarterly vulnerability scans. Internal scans would need to be**
- No **performed by the customer if needed.**

[PCI DSS v4.0 PDF](#)

Is segmentation used to isolate the cardholder data environment (CDE) from other networks? If so, are penetration tests performed on segmentation controls as follows?

- At least once every 12 months and after any changes to segmentation controls/methods.
- Covering all segmentation controls/methods in use.
- According to the entity's defined penetration testing methodology.
- Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems.
- Confirming effectiveness of any use of isolation to separate systems with differing security levels (Only one primary function exists on a system component, OR primary functions with differing security levels that exist on the same system component are isolated from each other, OR primary functions with differing security levels on the same system component are all secured to the level required by the function with the highest security need).
- Performed by a qualified internal resource or qualified external third party.
- Organizational independence of the tester exists (not required to be a QSA or ASV)

- Yes **Cardholder data is not stored in ChiroSpring or its servers. We store a secure token only.**
- No **It is up to the customer to ensure their software/cardholder data environment (CDE) is on a separate network from other applications in the office.**

[PCI DSS v4.0 PDF](#)

A change-detection mechanism (for example, file integrity monitoring tools) is deployed as follows?

- To alert personnel to unauthorized modification (including changes, additions, and deletions) of critical files.
- To perform critical file comparisons at least once weekly.

- Yes **There are no alerts in ChiroSpring for altering or deleting a file. Use of audit logs. Only customer can answer this.**
- No **logs. Only customer can answer this.**

[PCI DSS v4.0 PDF](#)

Are all information security policies reviewed at least annually and updated as needed, and does that review include an annual process to identify threats and vulnerabilities, and does that review result in a formal, documented analysis of risk and is that risk assessment process performed at least annually and also upon significant changes to the environment (for example, acquisition, merger, relocation, etc.)? Note: PCI ToolKit users will be given updated policies when performing their annual update.

- Yes
- No **Only customer can answer this.**

[PCI DSS v4.0 PDF](#)

Is your information security policy reviewed at least once every 12 months and updated as needed to reflect changes to business objectives or risks to the environment?

- Yes
 - No
- Only customer can answer this.

[PCI DSS v4.0 PDF](#)

Does your security policy clearly define information security roles and responsibilities for all personnel, AND are all personnel aware of and acknowledge their information security responsibilities?

- Yes
- No Only customer can answer this.

Previous

[PCI DSS v4.0 PDF](#)

Are acceptable use policies documented for end-user technologies and include:

- Explicit approval by authorized parties.
- Acceptable uses of the technology.
- List of products approved by the company for employee use, including hardware and software.

Yes **Only customer can answer this.**
 No

[PCI DSS v4.0 PDF](#)

Are policies and procedures documented to define a process for performing targeted risk analyses for each PCI DSS requirement that provides flexibility for how frequently the requirement is performed, and that the process includes all elements specified below?

- Identification of the assets being protected.
- Identification of the threat(s) that the requirement is protecting against.
- Identification of factors that contribute to the likelihood and/or impact of a threat being realized.
- Resulting analysis that determines, and includes justification for, how frequently the requirement must be performed to minimize the likelihood of the threat being realized.
- Review of each targeted risk analysis at least once every 12 months to determine whether the results are still valid or if an updated risk analysis is needed.
- Performance of updated risk analyses when needed, as determined by the annual review.

Yes

No

Only customer can answer this.

Previous

[PCI DSS v4.0 PDF](#)

Is a formal security awareness program implemented to make all personnel aware of the entity's information security policy and procedures, and their role in protecting the cardholder data?

- Yes
- No **Only customer can answer this.**

[PCI DSS v4.0 PDF](#)

Does security awareness training include awareness of threats and vulnerabilities that could impact the security of the CDE, including but not limited to:

- Phishing and related attacks?
- Social engineering?

Yes

No

Only customer can answer this.

[PCI DSS v4.0 PDF](#)

Do you keep and maintain a list of all third-party service providers (TPSPs) with which account data is shared or that could affect the security of account data, including a description for each of the services provided?

- Yes
- No **Only customer can answer this.**

Previous

[PCI DSS v4.0 PDF](#)

Are your written agreements with third-party service providers (TPSPs) maintained as follows:

- Written agreements are maintained with all TPSPs with which account data is shared or that could affect the security of the Cardholder Data Environment (CDE)?
- Written agreements include acknowledgments from TPSPs that they are responsible for the security of account data the TPSPs possess or otherwise store, process, or transmit on behalf of the entity, or to the extent that they could impact the security of the entity's CDE?

- Yes **Only customer can answer this.**
- No

Previous

[PCI DSS v4.0 PDF](#)

Is there an established process implemented for engaging third-party service providers (TPSPs), including proper due diligence prior to engagement?

- Yes
- No **Only customer can answer this.**

[PCI DSS v4.0 PDF](#)

Is a program implemented to monitor third-party service providers' (TPSPs) PCI DSS compliance status at least once every 12 months?

- Yes
 - No
- Only customer can answer this.

[PCI DSS v4.0 PDF](#)

Is Information maintained about which PCI DSS requirements are managed by each third-party service provider (TPSPs), which are managed by the entity, and any that are shared between the TPSP and the entity?

- Yes
- No **Only customer can answer this.**

[PCI DSS v4.0 PDF](#)

Do you have an incident response plan that is ready to be activated in the event of suspected or confirmed security incidents which includes, but is not limited to, the following?

- Roles, responsibilities, and communication and contact strategies in the event of a suspected or confirmed security incident, including notification of payment brands and acquirers, at a minimum.
- Incident response procedures with specific containment and mitigation activities for different types of incidents.
- Business recovery and continuity procedures.
- Data backup processes.
- Analysis of legal requirements for reporting compromises.
- Coverage and responses of all critical system components.
- Reference or inclusion of incident response procedures from the payment brands.

- Yes **Only customer can answer this.**
- No

[PCI DSS v4.0 PDF](#)

Are specific personnel designated to be available on a 24/7 basis to respond to suspected or confirmed security incidents?

- Yes
- No **Only customer can answer this.**

[PCI DSS v4.0 PDF](#)

Where POS POI terminals at the merchant or payment acceptance location use SSL and/or early TLS, does the entity confirm the devices are not susceptible to any known exploits for those protocols?

- Yes
 - No
- ChiroSpring Pay provides updates to terminals automatically as needed.