fortis

Best Practices for Chiropractic Clinics

Chargeback Prevention & Response

This guide is designed to help offices proactively reduce the risk of chargebacks while ensuring they have the appropriate documentation and processes in place to address disputes efficiently.

Enrollment & Authorization

(Required for care plans & recurring billing)

Obtain a **signed recurring payment authorization** for every care plan.

This should include the patient's name, last four digits of the card on file, payment schedule (amount and frequency), start and end dates, cancellation instructions, and a patient signature or electronic consent (e.g., DocuSign). Clearly indicate the **date the payment method** on file will be charged.

Bonus: Fortis includes built-in recurring payment authorization workflows to help ensure compliance and proper documentation.

For in-clinic enrollments, perform an **EMV chip read** for the initial authorization whenever a card is present and retain the associated authorization code.

Whenever possible, use tap or insert (EMV) instead of keyed or swiped transactions to reduce fraud risk.

Tokenize the card immediately after the initial authorization to securely store it for the future.

Provide **advance notice prior to any scheduled or recurring charges**, clearly indicating the billing date in all communications.

Bonus: Fortis allows you to customize the timing of automated email reminders sent to patients in advance of scheduled payments or appointments.

Use a **clear and recognizable merchant descriptor** that aligns with your clinic name and website on receipts and statements.

The statement descriptor is typically set to your **Doing Business As (DBA) name**. For questions or updates, please contact **support@fortispay.com**.

Booking, Cancellation & No-Show Policy

Maintain a **written cancellation and no-show policy** that is included in intake paperwork and on all booking pages. Obtain patient acknowledgment through a signature or electronic acceptance.

Ensure all signed or accepted documents include a **date and time stamp.**

Send **automated appointment reminders** via email and text at multiple intervals (e.g., 72 hours and 24 hours prior to the appointment). Communications should clearly include the **cancellation policy**, cutoff timeframe, and a direct **cancellation option** (link or phone number).

Maintain detailed, time-stamped records of all **cancellations and change requests**, including staff handling and communication method.

Accepting Payments – Fraud & Unauthorized Use Prevention

Avoid manually keyed or swiped card transactions whenever possible; use **EMV-enabled terminals** for in-person payments and require **CVV** for online transactions

For first-time card use, **verify the cardholder's identity** (where permitted by law) and document verification in the patient record

Use Fortis for secure tokenization and ensure all payment processing occurs within PCI-compliant systems

Send transaction receipts immediately to the cardholder via email to confirm payment details.

Bonus: Contact Fortis Support to enable automatic emailed receipts globally, eliminating the need to manually send receipts for each transaction.

Storage & Retention – Patient Records

Maintain **all supporting documentation** within the patient's billing record for easy access and reference.

Retain all documentation for a minimum of **24 months**, or longer if required by applicable regulations.

When to Void vs Refund a Payment

Void: Use when a transaction has not yet settled (same business day or prior to batch close).

For accounts on auto-batching, batches typically close at **9:30 PM** Eastern Time.

Refund: Use when a transaction has already settled or the void window has passed. Process refunds 48–72 hours within approval and notify the patient accordingly.

Always send the cardholder a confirmation via email for any void or refund, including the amount, transaction ID, and expected processing timeframe.

Bonus: When accessing a transaction in Fortis to process a void or refund, the system will only display the appropriate option based on the transaction status, helping reduce errors.

Representment Decision Workflow

If a customer contacts you with a service-related issue or misunderstanding, consider **issuing a prompt refund** to prevent a chargeback and associated fees

If a chargeback is filed, review the case to determine if **representment (challenging the dispute)** is appropriate based on available supporting evidence.

Do not issue a refund after a chargeback is filed, as the card issuer has already provided provisional credit

Compile all relevant documentation to create a strong **representment package.**

Submission timelines are typically within **14 days of the dispute date**, depending on the card network.

If representment is submitted, retain all original documentation and keep a record of the **submission confirmation** for your records.

Representment/Challenge Packet Requirements

Provide a **clear, factual timeline** of events with relevant timestamps.

Include **numbered supporting documentation**, referenced within the rebuttal. Typical evidence may include:

1. Signed recurring/payment authorization
2. EMV, 3DS, AVS, CVV, and authorization receipts, along with tokenization confirmation
3. Enrollment confirmations and reminder communications (email/SMS) with delivery records
4. Transaction receipt including authorization code
5. Treatment notes and patient check-in records
6. Shipping confirmation and proof of delivery (if applicable)
7. System audit logs reflecting staff actions
8. Cancellation records, if relevant

Prepare a **concise rebuttal statement** that clearly connects the supporting evidence to the dispute and formally requests a reversal.

EXAMPLE

Rebuttal Response Template – **Canceled Services**

The patient did not provide notice of cancellation prior to the scheduled appointment. In accordance with card network (Visa, Mastercard, American Express, Discover) guidelines, the cardholder is expected to attempt to resolve the matter directly with the merchant before initiating a dispute. At this time, there is no record indicating the patient contacted our office for resolution.

Per our policy, the services have now been canceled as of this notification. Supporting documentation, including time-stamped records of authorization, cancellation policy acknowledgment, appointment reminders, service delivery, and payment, is attached.

Attached Documentation:

- Signed intake/treatment plan and cancellation policy (including patient signature and date)
- Booking confirmation and reminder communications with delivery timestamps
- Check-in log and clinician treatment notes with timestamps and clinician initials
- Transaction receipt and authorization record (EMV, AVS, or 3DS data where applicable)
- Administrative cancellation entry created following receipt of the chargeback notification
- System audit log showing staff user ID and timestamp of transaction processing
- Additional communications confirming no prior cancellation request (if applicable)

Based on the signed authorization, transaction and authorization records, and documentation of services rendered, we respectfully request that this chargeback be denied and the transaction reinstated.

EXAMPLE

Rebuttal Response Template – **Fraud Claim**

This charge is not fraudulent. The patient has an established relationship with our clinic and authorized the transaction.

The cardholder scheduled and attended a chiropractic appointment on [Date], received services as documented in the attached treatment notes and invoice, and authorized payment through the signed intake and authorization forms. Check-in and check-out records further confirm the patient's presence at the time of service.

Attached Documentation:

- Records of prior visits and payments (appointment history and transaction receipts)
- Signed intake/treatment plan and cancellation policy (including patient signature and date)
- Dated treatment notes (SOAP notes)
- Booking confirmation and reminder communications with delivery timestamps
- Check-in log and clinician treatment notes with timestamps and clinician initials
- Transaction receipt and authorization record (EMV, AVS, or 3DS data where applicable)
- System audit log showing staff user ID and timestamp of transaction processing
- Additional supporting communications, if applicable

Based on the transaction and authorization records, along with documentation of services rendered, we respectfully request that this chargeback be denied and the transaction reinstated.

Best Practice for **Fraud Prevention**

Account Security (First Line of Defense)

- Use strong, unique passwords for all Fortis users
- Never share login credentials (internally or externally)
- Each Staff member running transactions should have their own individual user.
- Limit user access by role (only give refund/batch permissions to trusted personnel)
- Immediately deactivate users who leave the company

User & Permission Controls

- Restrict refund capabilities to a small, controlled group
- Regularly audit user access and permissions

Transaction & Refund Monitoring

- Understand and monitor your average daily transaction volume to quickly identify unusual activity.
- Review transactions and refunds daily to identify any suspicious activity (i.e. transactions—including refunds—that were not run by any office staff)
- Ensure daily batches are not manually closed before your location's auto-batch time

System & Network Security

- Use secure, trusted devices only to access Fortis
- Avoid public Wi-Fi when logging into the gateway
- Install antivirus/endpoint protection software
- Keep systems and browsers updated

Best Practice for **Fraud Prevention**

Phishing & Social Engineering Awareness

- Train staff to recognize phishing emails and fake support calls
- Never click unknown links or download suspicious attachments
- Verify any request for login access

Fortis Configuration Best Practices

- Enable AVS and CVV verification for transactions
- Set velocity controls or fraud filters (if applicable)
- Blind refunds should be disabled by default and only enabled when necessary
  1. They allow refunds without a linked original transaction
  2. They may be used for legitimate cases (e.g., returns without receipts), but increase risk
- Contact Fortis Support at **855-465-9999** to enable blind refunds on a case-by-case basis for refunds greater than 6 months or refunds without an offsetting sale

Incident Response Readiness

- Contact Fortis Support immediately at **855-465-9999** (call, don't chat)
- Document all suspicious transactions and timelines
- Immediately change passwords if suspicious activity is detected
- Admin users should disable affected user accounts right away
- Notify impacted patients/contacts if necessary

Ongoing Risk Management

- All merchants should enroll in Commerce Control Center to maintain visibility into their payment activity and keep a pulse on processing, disputes, reporting, and overall account health (commercecontrol.com)
- Perform regular internal audits of transactions and user activity
- Review chargeback and fraud trends monthly (create customized reports delivered to your email on a weekly/monthly basis)
- Update internal policies as new threats may emerge (refer to Account Security section above)