This Healthcare Website Privacy Policy explains how Kansas City Vascular Institute, LLC ("we", "us", "our") collects, uses, discloses, and protects personal information — including protected health information (PHI) — through our website KCVI.COM and related online services. This policy supplements our Notice of Privacy Practices and applies to information collected through the website, patient portal, online forms, telehealth services, and other electronic communications.

---

1. Scope and applicability

This policy applies to:

- Individuals who visit or use our website and online services
- Patients and prospective patients who provide information through online forms or via the patient portal
- Users of telehealth and appointment-scheduling tools hosted on or linked from our site

This policy covers both personal information and PHI as defined under HIPAA when such information is created, received, maintained, or transmitted by us in connection with healthcare services.

2. Definitions

- Personal Information: Information that identifies or can be used to identify an individual (e.g., name, email, phone number).
- Protected Health Information (PHI): Individually identifiable health information created, received, maintained or transmitted by a HIPAA-covered entity or its business associate in relation to healthcare services, treatment, payment, or operations.
- Business Associate: A service provider that creates, receives, maintains, or transmits PHI on our behalf and is contractually bound under a Business Associate Agreement (BAA).

3. Information we collect

We may collect the following types of information through the website and related services:

A. Contact & identity information

- Name, address, email, phone number
- Date of birth, gender

B. Health & medical information (may constitute PHI)

- Medical history, diagnoses, medications, treatment notes
- Allergy information, lab results, imaging reports
- Insurance and billing information

C. Appointment and scheduling data

- Appointment dates, clinician assigned, visit notes entered by clinicians

D. Payment and billing data

- Insurance provider, member ID, billing address, payment transactions (processed by third-party payment processors)

E. Technical and usage data

- IP address, device/browser type, pages viewed, referral URL, cookies and tracking identifiers

F. Communications

- Messages sent via the patient portal, email communications, telehealth session metadata (duration, timestamps) — note that telehealth content is PHI if it contains health information.

4. How we collect information

- Directly from you when you register, complete forms, communicate with us, or use the patient portal
- Automatically when you browse our site (cookies and analytics)
- From third parties, such as referring providers, insurance companies, labs, and vendors (including business associates)

5. Uses of information

We use personal information and PHI for the following purposes:

- Treatment: To provide, coordinate, and manage healthcare services, including telehealth visits and follow-up care
- Payment: To bill and obtain payment for services, verify insurance eligibility, and process claims
- Healthcare operations: For quality improvement, care coordination, practice management, auditing, training, and provider credentialing
- Communications: To contact you with appointment reminders, test results, updates, or other information related to your care
- Website functionality: To operate and maintain the website, manage accounts, and personalize content
- Legal and regulatory compliance: To comply with laws, respond to legal requests, and protect the safety of patients and staff
- Marketing and fundraising (only with your authorization): To send promotional materials or fundraising requests if you explicitly authorize us to do so

Where required by law or regulation (for example under HIPAA), we will only use or disclose PHI in accordance with that law. For uses beyond treatment, payment, and healthcare operations, we will obtain your written authorization where necessary.

6. Disclosures to third parties and business associates

We may disclose personal information and PHI to the following categories of recipients:

- Healthcare providers and clinical staff involved in your care
- Business associates who perform services on our behalf (e.g., EHR vendors, cloud hosting, telehealth platforms, billing companies). We require BAAs with such vendors where PHI is involved.
- Insurance companies and payers for payment and claims processing
- Public health authorities and others as required by law (e.g., reporting communicable diseases)
- Legal authorities in response to valid subpoenas, court orders, or other legal processes
- For research purposes, only when authorized by you or when the data is adequately de-identified in accordance with applicable law

We will not sell your PHI. To the extent applicable state law treats certain information as a sale (e.g., targeted advertising using certain identifiers), we will follow applicable opt-out rules.

7. Cookies, analytics, and tracking

We use cookies and similar technologies to provide website functionality, measure site performance, and analyze usage. Cookies fall into categories such as:

- Strictly necessary cookies for site functionality
- Functional cookies for preferences
- Analytics cookies (e.g., Google Analytics) to understand usage and improve the site
- Advertising and targeting cookies (only used where permitted and with consent if required by law)

We limit the inclusion of tracking in areas of the site that capture PHI when feasible. If you use the patient portal or enter health information, avoid enabling cross-site advertising or third-party trackers in your browser to reduce linkage of usage data to advertising profiles.

8. Telehealth and online communications

Telehealth sessions may be conducted using our telehealth vendor. These services collect metadata and may record session content only with patient consent. Telehealth platform vendors that handle PHI will be Business Associates and subject to a BAA. Avoid transmitting highly sensitive information via unsecured email.

9. Security measures

We implement administrative, technical and physical safeguards to protect personal information and PHI, including but not limited to:

- Access controls and user authentication for staff and patients
- Data encryption in transit (e.g., TLS/HTTPS) and at rest where practicable
- Regular security assessments, logging, and monitoring
- Employee training on privacy and security

Despite these measures, no electronic transmission or storage system is completely secure. If you suspect unauthorized access to your account, contact us immediately at the address below.

10. Data retention

We retain personal information and PHI as required for treatment, payment, healthcare operations, and to meet legal or regulatory obligations. Retention periods vary by record type and jurisdiction. Typical guidelines:

- Clinical records: retained in accordance with professional and state law (commonly 7–10 years after last encounter, or longer for minors)
- Billing records: retained for legal and tax compliance (commonly 7 years)
- Website analytics: aggregated and/or retained for a shorter period (e.g., 12–24 months)

We securely dispose of or de-identify information when it is no longer needed.

11. Your rights

Subject to applicable law and verification procedures, you may have the right to:

- Access and obtain a copy of PHI in our records
- Request an amendment of PHI (if inaccurate or incomplete)
- Request an accounting of disclosures of PHI
- Request restrictions on certain uses and disclosures of PHI (we are not required to agree to all requests)
- Request confidential communications (e.g., alternate contact method)
- Revoke authorizations for future uses/disclosures (does not affect disclosures already made)
- Where applicable (e.g., GDPR or CCPA/CPRA): request deletion, data portability, and opt-out of certain processing activities

To exercise your rights, contact: infor@kcvi.com or 5320 College Blvd., Leawood, KS 66211. We may require identity verification and will respond within the time frames required by law.

12. Breach notification

If we discover a breach of unsecured PHI as defined under HIPAA, we will follow breach notification requirements, which may include notifying affected individuals, the Secretary of

HHS, and, where applicable, the media and state regulators. We will also take steps to contain and mitigate the breach.

13. Minors

Our site and services are not directed at children under the applicable minimum age (typically 13 in the U.S. or as otherwise required by local law). We do not knowingly collect PHI from minors without parental or guardian consent. If we learn we have collected information from a minor in violation of law, we will take steps to remove it.

14. International transfers

If personal information or PHI is stored or processed outside your jurisdiction, we will implement appropriate safeguards (e.g., Standard Contractual Clauses, local law assessments) and comply with cross-border data-transfer requirements where applicable.

15. Third-party links and embedded content

Our website may contain links to third-party websites (e.g., labs, payers, telehealth vendors). This policy does not apply to those sites. Review the privacy policies of any third-party sites you use.

16. Changes to this policy

We may update this policy to reflect changes in law, technology, or our practices. We will post the revised policy with a new "Last updated" date. For material changes affecting how we use PHI, we will provide notice as required by law.

17. Contact information

Privacy Officer: Emily Carlson
Email: info@kcvi.com
Phone: 913-529-8600
Mailing address: 5320 College Blvd, Leawood, KS 66211

For HIPAA-specific complaints, you may also contact:

- U.S. Department of Health & Human Services, Office for Civil Rights: https://www.hhs.gov/ocr

---