Mid Florida Privacy Practices



Effective October 2026

Purpose

This Website Privacy Policy ("Policy") describes how Mid Florida Cancer Centers collects, uses, discloses, and safeguards personal information through our public website and related online services (collectively, the "Website").

This policy is intended to comply with applicable federal and state privacy laws, including where applicable comprehensive state consumer privacy statutes.

This policy does not replace or modify our HIPAA Notice of Privacy Practices (NPP), which governs how we use and disclose protected health information (PHI) for patients receiving medical care.

Enterprise Alignment & Website Scope

Mid Florida Cancer Centers is an affiliated physician practice operating as part of the OneOncology network, which provided administrative and operational support services to physician practices.

This Privacy Policy applies solely to personal information collected through this Practice's Website.

OneOncology maintains a separate Privacy Policy applicable to its corporate website and enterprise-level operations. Nothing in this Policy modifies or replaces:

- The OneOncology corporate website privacy policy
- The Practice's HIPAA Notice of Privacy Practices

For clarity:

- The Practice is the HIPAA-covered entity responsible for patient care and protected health information
- This Policy governs Website-collected personal information only
- Information collected through other systems (e.g., EHRs, patient portals, billing systems) is governed by separate policies and applicable law

Scope & HIPAA Clarification

This policy applies only to personal information collected through the Website.

Information submitted through the Website may become PHI if it is received, maintained, or used in connection with the provision of healthcare services. Once information becomes PHI it is governed by HIPAA and our NPP.

We do not intentionally collect PHI through the Website except through secure, designated channels (e.g., patient portals or secure intake tools).

Users are advised not to submit sensitive health or medical information through general contact forms, standard email, or other unsecured communication channels.

Personal Information We Collect

In the preceding twelve (12) months, we have collected the categories of personal information described in this section.

Categories	Examples	Purpose of Collection
Identifiers	Name, email address, phone number, IP address	Respond to inquiries, scheduling, communications
Internet/Network Activity	Pages visited, browser type, device data, referring URLs	Website functionality, analytics, security
Geolocation Data	General location derived from IP address	Security, analytics
Communications	Information submitted via forms or inquiries	Respond to requests, provide services

We do not knowingly collect or process sensitive personal information for purposes of targeted advertising, profiling with legal or similarly significant effects, or secondary commercial purposes.

Sources of Personal Information

We collect personal information from the following sources:

- Directly from you
- Automatically through cookies, pixels, and similar technologies
- From service providers hat support website functionality, analytics, and security

How We Use Personal Information

We process personal information only as reasonably necessary and proportionate to achieve the purposes for which it was collected, consistent with applicable law.

We do not process personal information for purposes that are materially different, unrelated, or incompatible with disclosed purposes without providing required notice and obtaining consent where required.

We use personal information to:

- Respond to inquiries and appointment requests
- Operate, maintain, and improve our Website
- Communicate regarding services and updates
- Protect the security and integrity of our systems

- Comply with legal and regulatory obligations
- Support business operations, including corporate transactions

Cookies and Tracking Technologies

We use cookies, pixels, web beacons, and similar tracking technologies support Website functionality, security, and analytics.

These technologies may collect information such as IP addresses, browser types, device characteristics, pages visited, time spent on pages, and referring URLs.

Certain analytics or advertising-related technologies may be considered "targeted advertising" or "sharing" under applicable state privacy laws.

We implement controls designed to prevent the collection or disclosure of protected health information ("PHI") through tracking technologies. Tracking technologies are not intentionally deployed or authenticated patient portal environments or on pages where users enter medical or health-related information.

Third-party vendors providing analytics or related services act on our behalf pursuant to contractual obligations designed to safeguard personal information.

Where required by law, we:

- Provide cookie consent and preference management tools
- Recognize Global Privacy Control (GPC) or similar universal opt-out signals
- Allow users to opt out of certain tracking activities

Users may also manage cookies through their browser settings; however, disabling cookies may impact Website functionality.

Disclosure of Personal Information

We may disclose personal information to:

- Service providers (e.g., hosting, analytics, IT security)
- Professional advisors (e.g., legal, accounting)
- Government authorities when required by law
- Successors in connection with a merger, acquisition, or reorganization

We do not sell personal information for monetary consideration.

However, certain disclosures involving cookies or tracking technologies may be considered "sharing" or "targeted advertising" under applicable state privacy laws. Where required, individuals may opt out of such activities.

Data Retention

We retain personal information only for as long as reasonably necessary to fulfill the purposes described in this Policy, unless a longer retention period is required or permitted by law.

Retention determinations are based on:

- The nature of the information
- The purposes for which it was collected
- Legal and regulatory requirements
- Operational and security needs

We maintain internal data retention and disposal practices designed to support compliance with applicable laws.

Data Security

We implement reasonable administrative, technical, and physical safeguards designed to protect personal information from unauthorized access, disclosure, alteration, or destruction.

No method of transmission over the internet or electronic storage is completely secure; therefore, we cannot guarantee absolute security.

Your Privacy Rights

Depending on your state of residence, you may have rights regarding your personal information, including:

- Right to access personal information
- Right to correct inaccurate personal information
- Right to delete personal information
- Right to opt out of targeted advertising or “sharing”
- Right to limit use of sensitive personal information (where applicable)
- Right to appeal a denial of a privacy request (where applicable)
- Right to designate an authorized agent (where applicable)

To exercise your rights, please contact us using the information below. We will verify your identity as required by law prior to processing requests.

We will respond within timeframes required by applicable law. Where permitted, we may deny requests that are unfounded, excessive, or otherwise not required to be fulfilled under applicable law.

Children's Privacy

Our Website is not directed at children under 13 years of age, we do not knowingly collect personal information from children.

Third-Party Links

Our Website may contain links to third-party websites. We are not responsible for the privacy practices or content of those external sites.

Sensitive Data & Profiling

We do not process sensitive personal data for purposes of profiling in furtherance of decisions that produce legal or similarly significant effects concerning consumers.

Changes to This Policy

We review this Policy at least annually and update it as necessary to reflect changes in legal requirements, technology, and business practices.

Material changes will be posted on the Website with an updated effective date.

Do Not Sell or Share/ Opt-Out Rights

Where required by applicable law, you may opt out of the sale or sharing of personal information or the use of personal information for targeted advertising.

You may exercise this right by:

- Submitting a request using the contact information below, or
- Using available opt-out mechanisms provided on the Website

We also recognize browser based opt-out signals, such as Global Privacy Control (GPC), where required by law.

If you have questions about this Policy or our privacy practices, please contact:

Mid Florida Cancer Centers

2776 Enterprise Road, Suite 100

Orange City, FL. 32725

Phone: 386-774-1223

Email: admin@mfhoc.com

Florida

Florida law provides certain protections related to data security and breach notification. While Florida does not currently provide comprehensive consumer privacy rights equivalent to other states, we apply consistent privacy practices across jurisdictions.