DIGITAL SERVICES PRIVACY POLICY

THIS DOCUMENT EXPLAINS OUR POLICIES AND ONLINE INFORMATION PRACTICES AND THE CHOICES YOU CAN MAKE ABOUT THE WAY YOUR INFORMATION IS COLLECTED AND USED BY ONLINE OR MOBILE WEBSITES, APPLICATIONS OR DIGITAL SERVICES OWNED OR OPERATED BY WAKE RADIOLOGY

Wake Radiology Privacy Policy:

This Privacy Policy explains our policies and online information practices and the choices you can make about the way your information is collected and used by online or mobile websites, applications, or digital services owned or operated by Wake Radiology ("Wake Radiology," "we," "us," or "our"). It applies to any online or mobile website, application, patient portal, or digital service on which this policy appears (each a "Service," collectively the "Services"). "Users" are persons who use the Services.

Certain subdomains of the Wake Radiology website are directed to providers and are subject to separate privacy policies. In addition, for information about Wake Radiology privacy policies and practices for handling patient protected health information (PHI), please see our HIPAA Notice of Privacy Practices here: https://www.wakerad.com/about/privacy-policy/. The HIPAA Notice governs how we create, receive, maintain, and transmit PHI in connection with care delivery and payment and remains separate from this policy.

By using the Services, you accept this Privacy Policy and consent to the practices described.

I. Information We Collect

We receive both information that is directly provided to us and information that is passively or automatically collected. We refer to personal information collected from you as the "Information."

A. *Information You Provide To Us.* At some Services, you can register, request appointments, obtain services, subscribe to newsletters, enter contests, vote in polls, participate in forums or communities, or otherwise express an opinion. We may collect name, address, email address, telephone number, and other details you choose to provide to fulfill your request.

   You may also submit Information about other people (e.g., to send gifts, cards, invitations, or emails). We will use such information only to fulfill your request and will not store it beyond what is necessary to fulfill that request.

B. *Information Automatically Collected.* We and our service providers may use cookies, pixels, web beacons, SDKs, locally stored objects, and similar technologies to collect information about your use of the Services and the device you use to access them (e.g., IP address, device identifiers, browser

type, pages viewed, time of visit, referring/exit pages). Some of this information may be personal information under state privacy laws and, in certain contexts for regulated entities, may constitute PHI under HIPAA.

C. *Information From Third Parties.* We may receive information about you from third-party sources (e.g., appointment referral systems, analytics providers, or social media platforms) to enhance our ability to serve you, tailor content, and offer opportunities we believe may be of interest. If we combine such data with Information collected via the Services, the combined data is subject to this Privacy Policy unless we indicate otherwise.

D. *Geo-location Information.* If you access a Service from a mobile device or through a mobile application, you may be asked to share geo-location data so we can customize your experience. You can disable geo-location collection at any time by changing your device or app privacy settings.

E. *Information Collected Through Social Media or Other Third-Party Platforms.* You can engage with our content on or through social media services or other third-party platforms. When you do, we may receive certain information you make available on those platforms. Your use of those platforms is subject to their respective privacy policies; we do not control those platforms' data practices.

II. How We Use the Information We Collect

We may use the information to:

- provide and communicate with you about the Services or your account;
- fulfill your requests regarding services (including appointment scheduling, newsletters, notifications);
- respond to inquiries and, where applicable, notify you if you have won a contest;
- communicate with you about other products, programs, or services we believe may be of interest to you (subject to your choices in Section V);
- conduct internal data analysis to improve the Services;
- enforce the legal terms that govern your use of the Services and/or the purposes for which you provided Information;
- provide technical support;
- prevent, detect, investigate, and respond to fraud or potentially illegal activities and maintain the security and integrity of the Services;
- customize or personalize offers and content based on your use of the Services;
- perform analytics regarding how you use the Services to improve our online communications and services;
- send gifts, cards, invitations, or emails to designated recipients, if you use such features.

Where the Information we process is PHI, we will handle it in accordance with HIPAA and our HIPAA Notice of Privacy Practices.

III. Information Sharing and Disclosure

We may disclose Information:

- To trusted service providers engaged to perform business-related functions on our behalf; where PHI is involved, by Business Associate Agreements (BAAs) as required by HIPAA.
- In response to legal process (e.g., court orders, subpoenas, law enforcement requests).
- To protect people, our organization, or the Services, including to investigate suspected illegal activities or security incidents.
- In connection with a business transition such as a merger, acquisition, or sale of assets, subject to applicable law and your rights.
- For state consumer privacy compliance, where required by law; we honor browser-based opt-out preference signals such as Global Privacy Control (GPC) as a valid request under California law.

IV. Online Tracking, Analytics, and HIPAA

A. *Cookies, Pixels, and Similar Technologies.* We use these tools to operate the Services, enhance user experience, conduct analytics, and (where permitted) measure marketing. Where these tools collect or receive PHI (for example, via authenticated patient portal pages or forms), disclosures must comply with HIPAA, including BAAs and permitted purposes, or require patient authorization.

B. *OCR Guidance on Tracking Technologies.* OCR has reminded regulated entities that HIPAA rules apply when tracking technologies collect or disclose PHI. A federal court vacated a portion of OCR's guidance regarding unauthenticated webpages; we will continue to assess our tracking practices and treat information as PHI where context indicates a connection to identifiable health information subject to HIPAA.

C. *Analytics Tools.* We may use analytics services to understand how visitors use the Services. Where analytics providers receive PHI, we will implement HIPAA-compliant safeguards (including BAAs) or obtain appropriate authorization.

D. *Do Not Track and Universal Opt-Out Signals.* While the legacy Do Not Track browser setting is not standardized and our Services do not respond to it, we honor Global Privacy Control (GPC) and other valid opt-out preference signals where required by law. If we engage in selling or sharing personal

information, we will provide a Do Not Sell or Share link and honor GPC signals as a valid opt-out.

V. Your Choices and Rights

A. *Access and Amendment.* To request access or correction, contact us (see Section XII). For PHI, please refer to our HIPAA Notice of Privacy Practices and designated channels for medical record requests.

B. *Marketing Communications.* To opt out of marketing emails, follow the unsubscribe instructions or contact us. We may still send transactional or service-related communications.

C. *Cookies and Targeted Advertising.* You can manage cookies via your browser settings. In states that grant opt-out rights for targeted advertising or sharing, we will provide methods to opt out, including honoring GPC signals.

VI. Children's Privacy

Our Services are intended for a general audience and are not directed to children under 13. If any portion is child-directed or has actual knowledge of collecting personal information from children under 13, we will comply with COPPA, including obtaining verifiable parental consent and meeting updated obligations such as separate opt-in consent for third-party disclosures and targeted advertising, data minimization, and retention limits.

VII. Automated Decision-Making and Profiling

We do not use Automated Decision-Making Technology (ADMT) to make clinical or treatment decisions via the Services. If we use ADMT to make or substantially replace human judgment in significant decisions, we will provide clear pre-use notices and offer opt-out rights as required under California CPPA regulations.

VIII. Data Security

We have implemented reasonable administrative, technical, and physical safeguards designed to protect Information, including ePHI. Our safeguards align with HIPAA Security Rule requirements and reference NIST SP 800-66 Rev. 2 to support risk analysis, risk management, access controls, encryption, logging, incident response, and workforce training.

IX. Data Retention and Minimization

We retain Information only for as long as necessary to fulfill the purposes for which it was collected, comply with legal obligations, resolve disputes, and enforce agreements. For COPPA-covered data, retention is limited to what is reasonably necessary and then

deleted securely. For certain state laws (e.g., CPRA), we disclose retention periods or criteria and limit use of sensitive personal information.

X. International Transfers

If personal data is transferred across borders, we will implement appropriate safeguards required by applicable law (e.g., EU Standard Contractual Clauses) and provide additional information to affected users where required. For EU/EEA health data, transfers will rely on lawful bases and appropriate safeguards consistent with GDPR Article 9.

XI. Breach Notification

We will investigate suspected or actual security incidents and, where a breach of unsecured PHI occurs, provide notifications to affected individuals, HHS OCR, and (if applicable) media without unreasonable delay and in no case later than 60 days from discovery, consistent with the HIPAA Breach Notification Rule. For non-HIPAA personal information, we will follow applicable state or international breach notification laws.

XII. Your Privacy Contacts

Marketing Director
Wake Radiology
3949 Browning Place, Raleigh, NC 27609
Email: marketing@wakerad.com

Privacy Officer
Carmen Geerlings, Corporate Compliance Officer
Wake Radiology
3949 Browning Place, Raleigh, NC 27609
Telephone: 919-787-7411 | Fax: 919-789-4461

XIII. Updates to This Privacy Policy

This Digital Services Privacy Policy is effective as of the date noted above. We may update this Privacy Policy from time to time. Material changes will be communicated by email (if you have provided one) and/or by posting a prominent notice on the Services. Please review this Policy periodically to understand our current practices. We encourage you to periodically check back to review this policy so that you always know what information we collect, how we use it, and with whom we share it.

XIV. Additional Notices (State-Specific and Washington MHMDA)

- California/CPRA: We will disclose categories of personal information collected, purposes, categories disclosed to service providers/contractors, retention, and provide rights forms (access, correction, deletion, opt-out of selling/sharing, limit use of sensitive personal information). We will honor Global Privacy Control

signals and, if applicable, provide a “Do Not Sell or Share My Personal Information” link.

- Colorado/Connecticut/Virginia/Utah: We will provide opt-out for targeted advertising and certain profiling, and methods to exercise data rights consistent with those laws, including recognition of universal opt-out signals where required.
- Washington MHMDA: Where applicable, we will publish a standalone Consumer Health Data Privacy Notice via a separate and distinct link on relevant pages, describing collection, use, sharing, and rights for consumer health data outside HIPAA.

Original Effective Date: November 15, 2016

Latest Revision Date: January 5, 2026