

PRIVACY POLICY

Last Modified: January 14, 2017

Effective Date: January 14, 2017

Rimage Solutions cares about privacy issues and wants you to be familiar with how we collect, use and disclose Personally Identifiable Information you provide to us through our website at www.carechatz.com ("Website") and our mobile app, **CareChatz** (the "Mobile App", together with the website as the "Services").

This Policy does not apply to the practices of companies that we do not own or control, or to individuals whom we do not employ, including any of the third parties to whom we may disclose user information as set forth in this Privacy Policy.

If you have any questions or comments about this Privacy Policy or our privacy practices, you may contact us at by mail at:

Attn: General Counsel
Rimage Solutions
124 Seven Oaks Dr.
Mulberry, FL 33860

By using the Services, you agree with all of the terms of this Privacy Policy. If you do not agree to this Privacy Policy, then please do not use the Services and, if you have installed the Mobile App, please uninstall it.

In the event you believe that your user id, password, device, or your access to the Service was compromised, you must notify our Security Officer immediately by e-mail at connect@rimagesolutions.net, subject: Attn: Security Officer.

1. PERSONALLY IDENTIFIABLE INFORMATION WE MAY COLLECT

"Personally Identifiable Information" is information that identifies you as an individual, such as name, postal address (including billing and mailing addresses), telephone number, e-mail address, or unique device identifiers.

- **We may collect Personally Identifiable Information in a variety of ways, including when:**
 - You contact us to request information by sending us an e-mail;
 - You download, install, and login into our Mobile App;
 - Your hospital or practice registers your Personally Identifiable Information for receiving the Services;
 - You use the Mobile App to send messages, via text or otherwise, to others using the Services;
 - You register for a webinar, CLE, to receive our newsletter, or other service through our Website;
 - You submit comments to us through a contact form or discussion board; or
 - You participate in a survey, contest, or other promotion.

- **We may use Personally Identifiable Information:**
 - To keep a record of your contact information and correspondence, and use it to respond to you, if you contact us through the Services;
 - To send administrative information, such as information regarding the Services and changes to our terms, conditions, or policies;
 - To respond to your inquiries and fulfill your requests;
 - For our business purposes, such as improving or modifying our Services, identifying usage trends, and operating and expanding our business activities;

- If you enter into a contest or similar promotion we may use the information you provide to administer those programs;
 - We may use survey information for research and quality improvement purposes, including helping us to improve information and services offered through the Services and we may, with your permission, contact you for follow-up if you specifically requested or based on the concerns you raised during the course of the survey;
 - As we believe to be necessary or appropriate: (1) under applicable law; (2) to comply with legal process; (3) to respond to requests from public and government authorities; (4) to enforce our terms and conditions; (5) to protect our operations against, for example, security threats, fraud or other malicious activity; (6) to protect our rights, privacy, safety or property, and/or that of you or others; and (7) to allow us to pursue available remedies or limit the damages that we may sustain.
- **Your Personally Identifiable Information may be disclosed:**
 - To identify you to anyone to whom you send messages through the Services;
 - To a hospital, practice, and other medical professional(s) using the Services;
 - To our third-party service providers that provide services such as website hosting, information technology and related infrastructure, customer service, email delivery, analytics, and other similar services;
 - To a third-party in the event of any reorganization, merger, sale, joint venture, assignment, transfer or other disposition of all or any portion of our business, assets or stock.
 - As we believe to be necessary or appropriate: (1) under applicable law; (2) to comply with legal process; (3) to respond to requests from public and government authorities; (4) to enforce our terms and conditions; (5) to protect our operations; (6) to protect our rights, privacy, safety or property, and/or that of you or others; and (7) to allow us to pursue available remedies or limit the damages that we may sustain.
- **California Do Not Track Notice:**
 - We do not track you over time and across third party websites to provide targeted advertising and therefore do not respond to Do Not Track (DNT) signals.
 - Third parties that have content embedded on the Website such as social networking connectors and advertising banners, may set cookies in your browser as well as obtain information about the fact that a web browser visited the Services from a certain IP address.

2. OTHER INFORMATION WE MAY COLLECT

“Other Information” is any information that does not reveal your specific identity or does not directly relate to an individual, such as: (1) computer and device connection information, such as browser type and version, operating system type and version, device information, and other technical identifiers; (2) information collected through cookies and other technologies; (3) demographic information and other information provided by you; or (4) aggregated information, such as usage history, search history, and types of procedures performed.

If we combine Other Information with Personally Identifiable Information, the combined information will be treated as Personally Identifiable Information for as long as it remains combined.

- **How We May Collect Other Information**

We, and our third-party service providers, may collect Other Information in a variety of ways, including:

- *Through your browser or mobile device:* Certain information is collected by most browsers or automatically through your mobile device, such as your computer type, screen resolution, operating system name and version, mobile device manufacturer and model, language, and Internet browser type and version.
- *Using cookies:* Our Services and advertisements may use cookies and other technologies such as pixel tags and web beacons. These technologies help us better understand user behavior, tell us which parts of our websites people have visited, and allow us to better

measure the effectiveness our marketing efforts. We treat information collected by cookies and other technologies as non-personal information. You have a variety of tools to control cookies and similar technologies, including controls in your browser to block and delete cookies.

- *IP Address:* Your “IP Address” is a number that is automatically assigned to the computer that you are using by your Internet service provider (ISP). An IP Address may be identified and logged automatically in our server log files, or those of our website hosting vendor, whenever a user accesses the Services, along with the time of the visit and the page(s) that were visited.
 - *By aggregating information:* Aggregated Personally Identifiable Information does not personally identify you or any other user of the Services. Aggregated Patient Health Information does not personally identify a patient or the provider that provided services to such patient. We may aggregate information for a variety of reasons, for example, to calculate the percentage of our users that live in a particular state, calculate the number of procedures performed in a particular state, or calculate the number of mobile app users.
- **How We May Use and Disclose Other Information**
 - We may use and disclose Other Information for any purpose, except where we are required to do otherwise under applicable law. If we are required to treat Other Information, such as IP addresses or other similar identifiers, as Personally Identifiable Information under applicable law, then we may use it as described in “*How We May Collect Other Information*” section above, as well as for all the purposes for which we use and disclose Personally Identifiable Information, but we will treat these identifiers as Personally Identifiable Information.

3. PATIENT INFORMATION AND SECURITY

(a) Patient Care Information

The Services may allow hospitals, practices, and providers to view and share their patients’ medical information, and professional services related information. This may include the names of patients to whom physicians will be providing services, the location and time of the procedures or care, and related matters. We acknowledge, and by using the Services, you acknowledge Patient Health Information, that the is subject to protection under the Health Insurance Portability and Accountability Act (“HIPAA”), the Health Information Technology for Economic and Clinical Health (“HITECH”), and their implementing regulations (collectively with HIPAA and HITECH, the “Privacy Laws”). We take reasonable administrative, technical, and physical security measures to protect the Patient Health Information. You acknowledge that you also have obligations under the Privacy Laws to protect the Patient Health Information by taking reasonable administrative, technical, and physical security measures and that you will take all such measures as needed to protect the Patient Health Information. You will also comply with your organization’s policies and procedures as may be related to your use of the Services and the Patient Health Information.

Patient Health Information is included in the definitions of Personally Identifiable Information. Patient Health Information will not be shared, disclosed, or sold to any third-party, except (1) as permitted by a Business Associate Agreement between us and a hospital or medical practice, (2) as permitted or required by the Privacy Laws, (3) in the event of any reorganization, merger, sale, joint venture, assignment, transfer or other disposition of all or any portion of our business, assets or stock as part of such transaction, or (4) in aggregated form as described in Other Information.

(b) Our Website

Our Website is divided into two components – a non-secured component (“General Website”) and the SSL encrypted administrative portal (“Extranet Portal”).

The communications on our General Website, including any submissions through available forms, are sent through the standard HTTP protocol and may be delivered using regular e-mail. Information sent over HTTP is not encrypted. E-mail, while convenient, also poses several risks (*e.g.*, e-mail is not a secure form

of communication, is unreliable, can be forwarded, etc.). We cannot guarantee the security of the information you provide to us through the General Website, nor can we guarantee that information you supply to us will not be intercepted while being transmitted to us. It is important for you to protect against unauthorized access to your computer and to take appropriate security measures to protect your information.

Please do not send any sensitive, confidential, or otherwise protected (e.g., Privacy Laws) information using regular e-mail.

(c) The Extranet Portal and the Mobile App

We take reasonable administrative, technical, and physical security measures to protect the data in the Website Extranet Portal and the Mobile App as required under the Privacy Laws and applicable Business Associate Agreements. Given the types of services being provided, you agree and acknowledge that you must also take reasonable administrative, technical, and physical security measures to protect the data in the Extranet Portal and the Mobile App by, for example, using secure Wi-Fi, protecting your password, locking your mobile device or your computer, and clearing any cached files.

In the event you believe that your password, device, or your access to the Service was compromised, you must notify our Security Officer immediately by e-mail at connect@imagesolutions.net, subject: Attn: Security Officer.

4. THIRD PARTY SERVICES

This Privacy Policy does not address, and we are not responsible for, the privacy, information or other practices of any third parties, including any third party operating any site or service to which the Services link. The inclusion of a link on the Services does not imply endorsement of the linked site or service by us or by our affiliates.

We are not responsible for the collection, usage and disclosure policies and practices of other organizations, such as your ISP, wireless service provider, the hospital, medical practice, or other providers using the Services.

5. CHOICES AND ACCESS

We may use your Personally Identifiable Information for marketing purposes such as to provide you the newsletters to which you subscribed, to advise you of contests and promotions, and to provide you details on upcoming events. You may opt-out of receiving these marketing messages by selecting the appropriate unsubscribe option included in the notice.

We may deliver sponsored ads to the Extranet Portal and the Mobile App. Your Personally Identifiable Information may be used to determine your potential level of interest in a sponsored ad or to otherwise provide the sponsored ad services. But, your Personally Identifiable Information will not be shared, sold, or otherwise disclosed to any third-party marketing company.

We may, from time to time, send you administrative messages. Because this information is important to your interaction with us, you cannot opt-out from receiving administrative messages.

6. USE OF SERVICES BY MINORS

We do not knowingly collect Personally Identifiable Information from individuals under the age of 13 and the Services are not directed to individuals under the age of 13. We request that these individuals not use the Services.

7. INTERNATIONAL VISITORS

The Services are controlled and operated from the United States, and are not intended to subject us to the laws or jurisdiction of any state, country or territory other than that of the United States. If any material on the Services is contrary to the laws of the place where you are when you access them, then we ask you not to use the Services. You are responsible for informing yourself of the laws of your jurisdiction and complying with them. By using the Services, you consent to the transfer of information to the United States, which may have different data protection rules than those of your country.

8. UPDATES TO THIS PRIVACY POLICY

We may change this Privacy Policy from time to time. Please take a look at the “Last Modified” legend at the top of this page to see when this Privacy Policy was last revised. Any non-material changes to this Privacy Policy will become effective when we post the revised Privacy Policy on the Services. When we change this Privacy Policy in a material way, we will either (1) post a notice on our Website along with the updated Privacy Policy, (2) push a notification about the changes to the Mobile App, or (3) send you an e-mail to the e-mail address we have for you with a link to the updated Privacy Policy. Your use of the Services following the non-material changes or 15 days after any material changes means that you accept the revised Privacy Policy.

9. CONTACTING US

If you have any questions about this Privacy Policy, you may contact us at by mail at Attn: General Counsel, Rimage Solutions, 124 Seven Oaks Dr., Mulberry, FL 33860.