



Notice of Privacy Rights

At Marque Medical, we recognize that you may be concerned about our use and disclosure of your personal information. Your privacy is very important to us and the following will inform you of the information that we, Marque Medical, may collect from you, and how it is used. By using our website, www.marquemedical.com, you are accepting the practices described in this policy. If, at any time, you have specific questions or concerns about the accessibility of any particular webpage, please contact info@marquemedical.com so that we may be of assistance.

If you feel that we not abiding by this privacy policy, you should contact us immediately via telephone at (877) 693-6266 or via mail Attn: Privacy Officer, 19900 MacArthur Blvd., Suite 800, Irvine, CA 92612.

Your privacy is as important to us as it is to you. Rest assured that any personal information you provide us with via this website, including your email address, will never be sold or rented to any third party without your expressed permission.

If you provide us with any personal or contact information in order to receive anything from us, we may collect and store that personal data.

Disclosures to Third Parties

1. In some instances, we may partner with a third-party partner to provide services such as newsletters, surveys to evaluate our services, health or company updates, and in such case, we may need to provide your contact information to third parties. This information, however, will only be provided to these third-party partners specifically for these communications, and the third-party will not use your information for any other reason.

Google Analytics

1. The Sites use Google Analytics, a web analytics service provided by Google, Inc. ("Google"). Google Analytics uses cookies or other Collection Technology to collect and store anonymous information about you, which may include the non-personally identifiable information described above. You can read Google Analytics' privacy policy at <http://www.google.com/privacy.html> and Google Analytics Terms of Use At <http://www.google.com/analytics/terms.us.html>
2. You can opt-out from being tracked by Google Analytics in the future by downloading and installing Google Analytic Opt-out Browser Add-on for your current web browser.



3. We do not automatically collect your personal email address simply because you visited our website. We may track the volume of visitors on specific pages and download information from specific pages, these numbers are only used as a whole and without personal information. This aggregate demographic information may be shared with our partners, but it is not linked to any personal information that can identify you or any visitor to our site.
4. We make every effort to secure any information submitted through our website, however, please be aware that any information you send via email may not be secure and we do not take responsibility for any information sent to us via email.

Privacy, Rights and Security: Marketing and Fundraising

1. Marque Medical is committed to safeguarding PHI (PHI Individually identifiable protected health information; data in motion, data at rest, data in use, data disposed (all forms, electronic, paper, and oral). Marque Medical may use or disclose PHI to inform patients of health-related benefits or services that may be of interest to them. Communication by Marque Medical or its business associates that directly or indirectly operate the business may include information on disease management, health promotion, preventative care, and wellness programs and may describe a health-related product or service (or payment for such product or service).
2. PHI may be used for marketing and fundraising purposes not covered by the HIPAA rule only when the recipient is notified prior. The recipient must be given a clear opportunity to opt out of receiving further marketing and fundraising communications.
3. A communication does not require an authorization, even if it is marketing or fundraising, if it is in the form of a face-to-face communication to an individual or a promotional gift of nominal value provided by the company.
4. Marque Medical may not sell PHI to a business associate or any other third party for that party's own purposes. Moreover, Marque Medical may not sell lists of patients to third parties in exchange for direct or indirect remuneration without obtaining authorization from each person on the list. If the marketing communication involves direct or indirect remuneration to the company from a third party, the authorization must state that such remuneration is involved.
5. In accordance with the HIPAA Privacy Rule, PHI will be considered de-identified health Information by Marque Medical only when specified by the "Expert De-Identification Method": A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:
 - a. Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information



- b. Documents the methods and results of the analysis that justify such determination.
6. Marque Medical's marketing and fundraising communications and activities will not be construed as amending, modifying, or changing any rule or requirement related to any other federal or state statutes or regulations, including specifically anti-kickback, fraud and abuse, or self-referral statutes or regulations, or to authorize or permit any activity or transaction currently proscribed by such statutes and regulations.

Facility Access Controls

1. The administrative team will ensure physical security measures to prevent unauthorized access to data, theft of data or the tampering of information system equipment by ensuring that only authorized personnel have access to electronic information systems.
2. Access to equipment, servers and network operations will be validated prior to use.
3. Visitors will be escorted and have appropriate authorization and supervision.

Acceptable Use and Security

1. All information systems are intended for business use only. Information system hardware, software and data will not be removed from the facility premises unless authorized for performing legitimate business. Laptops and PDA use will be authorized prior to system use.
2. Users will not intentionally introduce maliciousness into the information system and exercise caution when downloading files, opening emails and attachments, or other media from outside sources.

Unique User Identification

1. Usernames will be sensible, easily recognizable and have minimal potential for duplication.
2. Usernames shall reflect the employee name in some manner for ease of identification.
3. Each employee will be assigned a unique user account for identifying and tracking the employee use.

Password Protection

1. User shall have a unique password with minimum complexity and will have the option to prompt to change the password every 45 days.
2. Group and generic passwords will be prohibited except in the case where totally restricted access is involved or staff training exercises.
3. Password should not be written down in an unsecure manner and/or kept in an unsecure location near the workstation.
4. Passwords should be kept confidential by the user. Information Technology staff will have not had the ability to disclose passwords.

Device and Media Controls

1. Information Technology staff will manage the receipt, removal and movement of any hardware, storage device or media that contains electronic health or financial information and produce retrievable backup copies when indicated to limit the risk of damage or loss of data.



Software Controls

1. Only the Information Technology staff, or authorized contractors, consultants or vendors will install, maintain, uninstall or dispose of any software.
2. All software used will follow facility policies, licenses, copyright laws, contracts and agreements.
3. Movies, music and other copyrighted material may not be downloaded to facility computers.

Malicious Software Protection

1. Anti-virus software with current and automatic virus scanning is installed on all desktops, laptops, and servers.
2. Only Information Technology staff will isolate infected equipment and perform virus eradication.
3. All facilities must have latest versions of gateway intrusion prevention on their respective hardware.

Internet and Email

1. Use of internet, intranet and email will be suitable for business purposes and the normal execution of the employee job responsibilities.
2. All data on facility computer systems and network remain company property.
3. Facility administration may authorize the Information Technology staff to view or monitor emails, web sites, server logs, and electronic files or devices.
4. User access can be denied or revoked at any time for any reason.
5. Information Technology staff will utilize filtering software that is designed to block obscene internet sites or sites that do not have legitimate business value.
6. The Email Confidentiality Notice will accompany emailed information.

Faxing

1. Facsimile information contains important and confidential business information and will be handled accordingly.
2. Facsimiles will be sent with cover sheet containing pertinent facility information and a Fax Confidentiality Notice.

Security Review Process

1. Facility administrative team will per periodic risk assessment to review security measures and security policies annually to identify enough risks and implement security awareness and training.
2. Security reviews and evaluations will include technical and non-technical components.
3. All staff will participate in HIPAA training and comply with security requirements.
4. Privacy and Security Sanctions

Links on Our Site

1. Our site may contain links to other outside websites. We cannot take responsibility for the privacy policies or practices of these sites and we encourage you to check the privacy policies of all internet sites before you visit them.

Site Accuracy



1. While we make every effort to ensure that all information provided on our website is correct and accurate, we make no warranty, express or implied, as to the accuracy, completeness or timeliness, of the information available on our site. Marque Medical is not liable to anyone for any loss, claim or damages caused in whole or in part, by any of the information provided on our site.

Special Note to California Residents

California Civil Code Section § 1798.83 permits California residents that have provided any personal information through the sites the right to request certain information regarding our disclosure of personal information to third parties for their direct marketing purposes during the preceding year. We do not disclose personal information of customers to third parties for any third-party's direct marketing purposes. Please contact us at 615.600.4000 if you are a California resident and would to request information about how to exercise your third-party disclosure choices.

Non-Discrimination Notice

Marque Medical locations do not discriminate based on color, race, sex, national origin, age or disability in his health programs and activities.

Marque Medical locations provide free aids and services to people with disabilities to communicate effectively with us, such as qualified interpreters and information in alternate formats.

Marque Medical locations provide free language assistance services to people whose primary language is not English, including translated documents and oral interpretation, when necessary to provide meaningful access to our services.

If you need these aids or services and for further information, contact Marque Medical's HR Manager at 1-877-693-6266.

If you believe Marque Medical locations have failed to provide these services or discriminated in another way based on color, race, age, national origin, sex or disability, please contact Marque Medical's HR Manager at 1-877-693-6266.