Privacy Notice

941-776-4000
MCR.HEALTH

We maintain protocols to ensure the security and confidentiality of your personal health information (PHI). We have physical security in our building, passwords to protect databases, compliance audits and virus/intrusion detection software. Within our practice, access to your information is limited to those who need it to perform their jobs. Each employee is required to be trained in HIPAA rules and sign a consent form accepting responsibility for maintaining PHI.

At the offices of MCR Health, Inc., we are committed to treating and using protected health information about you responsibly. This Notice of Privacy Policies describes the personal information we collect and how and when we use or disclose that information. It also describes your rights as they relate to your protected health information. This Notice is effective March 26, 2013, with compliance enacted on September 23, 2013 and applies to all protected health information as defined by federal regulations. Changes have been made to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules, under the Health Information Technology for Economic and Clinical Health Act (HITECH) Mega rule and the Genetic Information Nondiscrimination Act.

Understanding Your Health Record:

Each time you visit MCR Health, Inc., your visit is noted in your record. Typically, this record contains your symptoms, examination/test results, diagnoses, treatment, and a plan for care or treatment. This information, often referred to as your health/medical record, serves as a:

- Basis for planning your care and treatment.
- Means of communication among the many health professionals who contribute to your care Legal document describing the care you received.
- Means by which you or a third-party payer can verify that services billed were actually provided source of data for medical research.
- Source of information for public health officials charged to improve the health of the state and nation source of data for our planning and marketing.
- Tool by which we can assess and continually work to improve the care we render and outcomes we achieve.

Understanding what is in your record and how your health information is used helps you to ensure its accuracy, to better understand who, what, when, where, and why others may access your health information and to make more informed decisions when authorizing disclosure to others. Electronic Health Records (EHR) is often used in practices instead of written paper. The EHR provides security, can be accessed by hospitals in an emergency, and ensure medications prescribed do not interact with other medicine(s). If our practice utilizes EHR, a notice of EHR digital record management system will be provided.

Your Health Information Rights:
Although your health record is the physical property of MCR Health, Inc., the information belongs to you.

You have the right to:

- Obtain a copy of this notice of privacy policies upon request. Request privacy protection for PHI (45 CFR§l64.522).
- Obtain and inspect a copy of your health record (reasonable copy fees apply in accordance with state law) Receive a copy (paper or electronic) of your PHI (45 CFR §164.524), within 30 days of signed request (digital signature can be utilized for EHR purposes).
- Amend your health record, which requires health care professionals to include your changes in your record. Obtain an accounting of disclosures of your health information, including who has requested your medical record Request confidential communications of your PHI.
- Request restriction(s) on certain uses and disclosures of your health information.
- Submit a complaint. If you believe your rights under privacy policies are being denied or your PHI is not being protected, you can file a complaint with the health care provider and the Office of Civil Rights.

For further information on HIPAA: www.hhs.gov/ocr/hipaa/
For HITECH Megarule information:
www.hhs.gov/ocr/privacy/hipaa/administrative/omnibus/

Our Responsibilities:
Our practice is a "Covered Entity" and we are required to:

- Maintain the privacy of your health information
- Ensure confidentiality, integrity, and availability of ePHI Create policies/procedures to maintain protection of PHI.
- Provide you with the notice as to our legal duties and privacy practices with respect to PHI we collect/maintain Abide by the terms of this notice.
- Notify you if there is a "breach" of your PHI, within 60 days Comply with your requested PHI restriction, including EHR. Accommodate requests you may have to communicate PHI Transmit health information in electronic form as necessary.
- We reserve the right to change practices and to make the new provisions effective for all PHI we maintain. We keep a posted copy of the current notice in our facility containing the effective date. In addition, each time you visit our facility for treatment, you may obtain a copy of the current notice in effect upon request. We will not use or disclose your health information in any manner, even as noted in the section Examples of Disclosures for Treatment, payment AND family/friend/personal representative without your authorization, which you may revoke, except to the extent that action has already been taken. In some situations, with your permission, a health care provider can share information with a family member or personal representative when he/she is either present or not present with you.

Are clients required to obtain authorization from the patient to release information to Phreesia?
No, the services Phreesia provides to the clients falls within the "health care operations" exception under HIPAA. Authorization from the patient is not required. The client however, must list in the Notice of Privacy Practices they distribute to their patients, situations with examples, such as "health care operations" in which the patient's authorization is not required for release of their information.

Breach of Personal Health Information:
Pursuant to 45 CFR parts 160 and 164, doctors, hospitals, and other health care providers, are required to inform you if there is a "breach" (unauthorized access/acquisition/use/disclosure) of your PHI. In cases of 500+ breached records, the Secretary of Health and Human Services is informed and notice given to media outlets in a state or jurisdiction of the breach.

For More Information or to Report a Problem:
If you have questions and would like additional information, you may contact our practice's Compliance Officer, Samida Johnson at
941-776-4000. If you believe your privacy rights have been violated, you can either file a complaint with the Office for Civil Rights, U.S. Department of Health and Human Services (OCR). There will be no retaliation for filing a complaint with either our practice or the OCR. The address for the OCR regional office for Florida is as follows: OFFICE FOR CIVIL RIGHTS
U.S. Department of Health and Human Services
Atlanta Federal Center, Suite 3B70
61 Forsyth Street, SW., Atlanta, GA 30303-8909

Committed to Protecting Your Identity
MCR Health trains staff on how to detect and report on fraudulent information.
In the event MCR Health engages a Service Provider to perform an activity, the organization will take steps to ensure the Service Provider performs its activities in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of Identity theft.

OTHER USEFUL RESOURCES ON IDENTITY THEFT:
Federal Trade Commission
(FTC)
www.consumer.gov/idtheft

U.S. Department of Justice
(DOJ)
www.usdoj.gov

U.S. Postal Inspection Service
www.usps.com/postalinspectors

Protecting Your Identity
Under recently issued regulations, the Federal Trade Commission re quires creditors to develop and implement written identity theft prevention programs. The broad purpose is to require creditors to formally address the risks of identity theft, the “Red Flags” and develop a mitigation plan. Health care providers can be creditors and subject to the rules.

The Red Flags Rule defines “Identity Theft” as “fraud committed using the identifying information of another person” and a “Red Flag” as a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.

Protecting Customer Identifying Information
In order to prevent the likelihood of identity theft occurring with respect to MCR Health , Inc. accounts, the organization will follow these steps with respect to its internal operating procedures to protect customer identifying information**:**

- Ensure that our website is secure or provide clear notice that the website is not secure
- Ensure complete and secure destruction of paper documents and computer files containing customer information
- Ensure that office computers are password protected and that computer screens lock after a set period of time
- Keep offices clear of papers containing customer information
- Ensure computer virus protection is up to date
- Require and keep only the kinds of patient information that are necessary for specific purposes

Prevent and Mitigate
In the event that a Red Flag is identified, MCR Health Inc., would take one or more of the following steps, depending on the degree of risk posed by the Red Flag:

- Continue to monitor accounts for evidence of Identity Theft
- Contact the patient
- Change any passwords or other security devices that permit access to ac counts
- Not open a new account
- Re-open an account with a new number
- Notify the Program Administrator for determination of the appropriate steps to take
- Notify law enforcement
- Determine that no response is warranted under the particular circumstances

Examples of Disclosures for Treatment, Payment, Family/Friend/Personal Representative, and Health Operations:

We will use your health information for treatment

We may provide medical information about you to health care providers, our practice personnel or third parties who are involved in the provision, management or coordination of your care.

For example: Information obtained by a nurse, physician, or healthcare provider will be recorded in your record and used to determine the course of treatment for you. Your medical information may be shared among healthcare professionals involved in your care.

We will use your health information for payment.

We may disclose your information so that we can collect or make payment for the healthcare services you receive. For example: If you participate in a health insurance plan, we disclose necessary information to that plan to obtain payment for your care.

We will use your health information for family/friend/personal representative.

We may disclose your information, as needed, to a family member, a friend or someone who is responsible for your care. For example: Following emergency surgery, you remain unconscious from the anesthesia and the surgeon informs your spouse of your condition.

We will use your health information for regular health operations.

We may disclose your health information for our routine operations. These uses are necessary for certain administrative, financial, legal, and quality improvement activities that are necessary to run our practice and support the core functions.

- Appointment reminders.
- We may disclose medical information to provide appointment reminders (e.g., contacting you at the phone number provided to us and leaving a message as an appointment reminder).
- Decedents.
- Consistent with applicable law, we may disclose health information to a coroner, medical examiner or funeral director.
- Public health.
- As required by law, we may disclose your health information to public health or legal authorities charged with preventing or controlling disease, injury or disability.
- Research
- We may disclose information to researchers when their research has been approved and the researcher has obtained a required waiver from the Institutional Review Board/Privacy Board, who has reviewed the research proposal.
- Organ procurement organizations.
- Consistent with applicable law, we may disclose health information to organ procurement organizations or other entities engaged in the procurement, banking or transplantation of organs for the purpose of donation and transplant.
- As required by law.

- We may disclose health information as required by law. This may include reporting a crime, responding to a court order, grand jury subpoena, warrant, discovery request, or other legal process, or complying with health oversight activities, such as audits, investigations and inspections, necessary to ensure compliance with government regulations and civil rights laws.
- Specialized government functions.
- We may disclose health information for military and veterans affairs or national security and intelligence activities.
- Business associates/sub-contractors.
- There are some services provided in our organization through contracts with business associates (BA) and sub-contractors, such as billing, data analysis, or transcription services. To protect your PHI (45 CFR§164.306), when these services are contracted the law requires the BA/sub-contractor (including EHR vendors) to appropriately safeguard your information, and as such must be compliant with all HIPAA privacy laws and security rules. If breaches occur with your PHI, the BA/sub contractor and the healthcare provider may be liable for HIPAA violations, which includes fines.
- Practice marketing.
- We may contact you to provide information about treatment alternatives or other health-related benefits and services that may be of interest to you (e.g., to notify you of any new tests or services that are being offered).
- Food and Drug Administration (FDA).
- We may disclose to the FDA health information relative to adverse events with respect to food, supplements, product and product defects, or post marketing surveillance information to enable product recalls, repairs or replacement.
- Personal representative.
- We may disclose information to your personal representative (person legally responsible for your care and authorized to act on your behalf in making decisions related to your health care).
- To avert a serious threat to health/safety and disaster relief.
- We may disclose your information when we believe in good faith that this is necessary to prevent a serious threat to your safety or that of another person. This may include cases of abuse, neglect, or domestic violence. Unless you object, we may disclose health information about you to an organization assisting in a disaster relief effort. For all non-routine operations, we will obtain your written authorization before disclosing your personal information.
- Communication with family.
- Unless you object to health professionals, using their best judgment, may disclose to family/personal friend health information relevant to that person's involvement in your care or payment related to your care. We may notify these individuals of your location and general condition.
- Genetic health information
- Genetic health information is also PHI. However, any genetic health information used for underwriting purposes is prohibited.
- Electronic Use of Personal Health Information (PHI).

- If we utilize Electronic Health Records (EHR), or other electronic method(s), we may transfer your health information electronically, as needed for payment, treatment, or health care operations, unless you request otherwise.
- Other Uses and Disclosures.

- **In the case we have other uses and disclosures not described herein, we will contact you and request your written authorization (45 CFR§l64.522**