NOTICE OF PRIVACY PRACTICES

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY

If you have any questions about this Privacy Notice, please contact Carri Riemer. This Notice of Privacy Practices is being provided to you as a requirement for the Health Insurance Portability and Accountability Act (HIPAA). This Notice describes how we may use and give out "disclose" your health information to carry out treatment, payment or heath care operations and for other purposes that are permitted or required by law. It also describes your rights to access and control your protected health information in some cases.

Treatment: We may use and disclose health information about you for the purpose of coordinating your health care. For example, we may need to disclose information to a case manager at a managed care organization who is responsible for coordinating your care.

Payment: We may use and disclose health information about you so that the services you receive can be properly billed and paid. For example, we may disclose your health information to permit your health plan to take certain actions before your health plan approves or pays for your services.

Operations: We may use or disclose health information about you, as necessary, so that we can operate the health plan and provide quality care to you. For example, we may use health information about you to review the quality of services you receive.

Other Uses and Disclosures: As part of treatment, payment and health care operations, we may also use or disclose health information about you so that we can send you healthcare service reminders and/or newsletters.

Federal privacy rules allow us to use or disclose your protected health information without your permission or authorization for a number of reasons. These reasons include the following:

- **When Required by Law**: We will disclose health information about you when we are required to do so by law.
- **When There Are Risks to Public Health:** For example, we may disclose your health information to prevent, control or report a disease.
- **To Report Abuse, Neglect or Domestic Violence**: We may notify government authorities if we believe that a patient is the victim of abuse, neglect, or domestic violence.
- **To Conduct Health Oversight Activities**: We may disclose your health information to a health oversight agency for activities such as audits or inspections.
- **In Connection With Judicial and Administrative Proceedings:** We may disclose your health information in the course of any judicial or administrative proceedings in response to an order of a court or administrative tribunal as expressly authorized by such order or in response to a signed authorization (in a format approved by the Michigan Court Administrator).
- **For Research Purposes:** We may use or disclose your health information for research under limited circumstances.
- **In the Event of A Serious Threat to Health or Safety**: We may use or disclose your health information if we believe, in good faith, that such use or disclosure is necessary to

prevent or lessen a serious and imminent threat to your health or safety or to the health or safety of the public.

- **For Specified Government Functions:** In certain circumstances, the Federal regulations authorize us to use or disclose your health information to facilitate specified government functions such as functions relating to national security.
- **For Worker's Compensation:** We may release your health information to comply with worker's compensation laws or similar programs.

Family Matters: Unless you object, or we can infer from the circumstances that you do not object, we may disclose your protected health information to your family member or a close personal friend if it is directly relevant to the person's involvement in your care or payment related to your care. We can also disclose your information in connection with trying to locate or notify family members or others involved in your care.

Authorization: Other than as stated above, we will not disclose your health information other than with your written authorization. You may revoke your authorization in writing at any time except to the extent that we have taken action in reliance upon the authorization.

Your Right to Inspect and Copy: You may request the right to inspect and get copies of your health information. To inspect and copy your health information, you must submit a written request to Carri Riemer, whose contact information is listed on the first page of this Notice. We can deny your request for certain limited reasons, but we must give you a written reason for denial. We may charge a fee for copying your records.

Your Right to Request a Restriction on Uses and Disclosures of Your Protected Health Information: You may ask us not to use or disclose certain parts of your health information for the purposes of treatment, payment or health care operations. We are not required to agree to a restriction. You may request a restriction by contacting Carri Riemer.

Your Right to Request Confidential Communications: You have the right to request that we communicate with you about health matters in a certain way or at a certain location. We will accommodate reasonable requests only if you notify us that disclosure of the health information could put you in danger. Requests must be made in writing to Carri Riemer. This written request must also contain a statement that disclosure of the information could endanger you.

Your Right to Amend: If you feel that the information we have about you is incorrect or incomplete, you may request that we amend your information. If we deny your request, we must give you a written reason for our denial. Requests must be made in writing to Carri Riemer. In this written request, you must also provide a reason to support the requested amendments.

Your Right to a List of Disclosures: You have the right to request a listing of certain disclosures of your health information. This right applies to disclosures for purposes other than treatment, payment or health care operations as described in this Notice of Privacy Practices. We are also not required to account for disclosures that you requested, disclosures that you agreed to by signing an authorization form and certain other disclosures that we are permitted to make without your authorization. The request for listing must be made in writing to Carri Riemer. We are not required to provide a listing of disclosures that took place prior to April 14th, 2003. We will provide the first listing that you request during any 12-month period without charge. Subsequent requests may be subject to a reasonable cost-based fee.

Your Right to a Copy of This Notice: You have the right to receive an additional copy of this Notice at any time. Even if you have already received a copy of the Notice or have agreed to accept this Notice electronically, you are still entitled to a paper copy of this Notice. Please call or write to Carri Riemer, whose contact information is listed on the first page of this Notice, to request a copy.

How to Use Your Rights Under This Notice: For any of the above requests that must be made in writing, we will help you prepare the written request if you need assistance. For assistance with a written request and for oral requests, please call Carri Riemer, whose contact information is listed on the first page of this Notice. Written requests can be sent to Carri Riemer at the address listed.

Our Duties: We are required by law to maintain the privacy of health information and to provide you with this Notice of our duties and privacy practices. We are required to abide by the terms of this Notice as may be amended from time to time. We reserve the right to change the terms of this Notice and to make the new Notice provisions effective for all health information that we maintain. If we make any major changes to our Notice, you will receive a copy of our new Notice within 60 days of the major changes.

Complaints: If you believe your privacy rights have been violated, you have the right to complain to us. You may complain to us by contacting Carri Riemer verbally or in writing. We encourage you to express any concerns you may have regarding the privacy of your information to us. You will not be retaliated against in any way for filing a complaint.
Contact Person: The contact person for all issues regarding the privacy of your health information is Carri Riemer.

ELECTRONIC COMMUNICATION RELEASE

Please complete the second page before returning

HIPPA (the Health Insurance Portability and Accountability Act) sets standards for protecting all patient information. Electronic communication makes HIPAA compliance more challenging, and it is important to acknowledge the possible risks inherent in these forms of communication. Doing so allows you make an informed decision about the types of commination that you are comfortable using.

1. Text / iMessage Communication
    a. Mobile SMS text messages are generally not secure because they lack encryption. Additionally, telecommunication vendors (including wireless carriers) may store text messages. Given these factors, it is possible for breaches of information to occur without the awareness of either party.

    b. Apple provides a higher level of encryption for individuals using iMessage. Each message sent to you is encrypted (AES-128), with different encryptions for each device you receive messages on. Some data, such as the timestamp and APN routing data is not encrypted. Both independently encrypted/non-encrypted data is encrypted as a whole package between your device and Apple's services, making it more difficult for others to decrypt. However, with a court order, Apple can add a public key into the mix, allowing messages sent after that point to be read by whoever has the corresponding private key.

    c. Regardless of the method of communication being used, it is important for individuals to be aware that breaches of security can also occur due to loss or theft of a computing device.

2. Cell Phone Communication. Communicating via cell phone provides an inherent risk, given the transmission is wireless. Accordingly, although cell phone use does not necessarily constitute a HIPAA violation, any phone calls from your mobile device and/or made to my phone number may be vulnerable to interception.

3. Email Communication. Please note that email communication is neither secure nor confidential, and may be intercepted between the sender and the receiver.

4. Video Based Telepsychology
    a. FaceTime. FaceTime has been said to comply with HIPPA regulations when users areconnected to a secure wireless network that is encrypted with WPA2 Enterprise security. In addition, each FaceTime session is encrypted end to end with unique session keys. Accordingly, once the connection between two Apple IDs is established, all communication is limited to the two recipients and does not pass through Apple's servers. The sessions are also encrypted so that the only people that can decrypt the transmission are the two parties conducting the call. Apple does not store any sessions nor to they have the ability to decrypt live FaceTime sessions. However, please note that when individuals are not using a secure wireless network, as noted above, there may be inherent risks to the security of the communication and the information exchanged.

ELECTRONIC COMMUNICATION RELEASE

I, _____(name / name of guardian – if under 18) _____(date of birth), have read this document in full and understand the inherent risks to using these forms of communication, given that the information exchanged may not be secure. I have read the first page of this document and, equipped with this knowledge, I consent to use of the following types of electronic confidentiality, despite the limits to communication noted above.

☐ Cell Phone _____ _____
Signature Date

☐ Mobile SMS Text Messages _____ _____
Signature Date

☐ iMessage _____ _____
Signature Date

☐ Email communication _____ _____
Signature Date

☐ FaceTime _____ _____
Signature Date

I have checked the boxes for each type communication that I have consented to using and have both signed and dated next to each of these approved means of communication.

_____ _____
Signature Date