eHEALTH GLOBAL TECHNOLOGIES, INC.
d/b/a
eHEALTH TECHNOLOGIES
250 Thruway Park Drive, West Henrietta, New York 14586

NOTICE OF PRIVACY PRACTICES
(Effective Date: April 14, 2003)

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 Notice of Privacy Practices please contact our Chief Privacy Officer - Michael A. Sciortino, Esq. at (877) 344-8999

This Notice of Privacy Practices has been modeled by the American Medical Association for use by covered entities and is consistent the Health Insurance Portability and Accountability Act of 1996, as codified at 42 U.S.C. §1320d *et seq*. ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act of 2009 ("HITECH Act") contained in Section 13402 of Title XIII of the American Recovery and Reinvestment Act of 2009 ("ARRA"), the Final Omnibus Rule, effective as of September 23, 2013, and describes how we may use and disclose your protected health information to carry out treatment, payment or health care operations and for other purposes that are permitted or required by law, and with regard to the specific services eHealth Global Technologies, Inc. d/b/a eHealth Technologies ("eHealth Technologies") provides to our customers including digital remote access to current systems, health information exchanges, and the digitizing and storage of outside images, records and reports. It also describes your rights to access and control your protected health information. "Protected health information" is information about you, including demographic information, that may identify you and that relates to your past, present or future physical or mental health or condition and related health care services.

We are required to abide by the terms of this Notice of Privacy Practices. We may change the terms of our notice, at any time. The new notice will be effective upon publication for all protected health information that we maintain at that time. Upon your written request to the Chief Privacy Officer, we will provide you with any revised Notice of Privacy Practices.

1. Purpose

This Notice of Privacy Practice applies to eHealth Technologies workforce members, including employees and related personnel, who are acting as a Business Associate of a Covered Entity or health

care provider who provides care for patients (such as physicians, physician assistants, therapists, and other health care providers who are not employed by eHealth Technologies). This Notice of Privacy Practices however, only details our privacy policies and how we will protect your protected health information. This Notice of Privacy Practices does not govern the independent practices or operations of any health care or service providers, such as the privacy practices that your doctor or hospital may use in their operations. eHealth Technologies may share your protected health information with a Covered Entity or other health care provider for their continued treatment of you, payment and health care operations in strict compliance with a Business Associate Agreement, HIPAA, HITECH Act, ARRA, and the Final Omnibus Rule. This arrangement is only for sharing information and not for any other purpose.

2. Choice and Consent

Prior to the collection of your personal and/or protected health information, eHealth Technologies will provide a written authorization to you for signature and approval, and identify the choices available to you with respect to the collection, use and disclosure of your personal and/or protected health information and that written permission is required to collect, use, and disclose personal and/or protected health information, unless a law or regulation specifically requires or allows otherwise, such as the continuity of care provisions of HIPAA. Your personal and/or protected health information is only being used for what you consented to at the time of collection. Additional consent will be requested, unless otherwise permitted or required by law as described herein, such as the continuity of care provisions of HIPAA.

You may revoke your consent in the authorization in writing at any time. If you revoke your consent for authorization, we will no longer use or disclose your personal and/or protected health information for the reasons covered by your written authorization. Please understand that we are unable to take back any disclosures already made with your prior consent/authorization. Please submit any written revocation of a written authorization to the Chief Privacy Officer at the address listed on the front of the Notice of Privacy Practices.

3. Collection

Your personal and/or protected health information is only collected for that which is necessary, for the purposes identified in this Notice of Privacy Practices. eHealth Technologies will only collect such personal and/or protected health information upon request of Covered Entity including your doctors or treating hospitals. We will not collect your personal and/or protected health information unless a request is directly made to us by you, or your doctor or treating hospital. The method and process by which your personal and/or protected health information is collected directly is reviewed by management and prior to its implementation is done in a fair and lawful manner.

4. Uses, Disclosures, and Retention of Protected Health Information

A. Uses:

For the purposes of providing health care services to you, your personal and/or protected health information may be used and disclosed by your physician, our office staff and others outside of our office. Your protected health information may also be used and disclosed to pay your health care bills and to support the operation of your physician's practice.

Following are examples of the types of uses and disclosures of your protected health information that your physician's office is permitted to make. These examples are not meant to be exhaustive, but to describe the types of uses and disclosures that may be made by our office.

Treatment: We will use and disclose your protected health information to provide, coordinate, or manage your health care and any related services. This includes the coordination or management of your health care with another provider. For example, we would disclose your protected health information, as necessary, to a home health agency that provides care to you. We will also disclose protected health information to other physicians who may be treating you. For example, your protected health information may be provided to a physician to whom you have been referred to ensure that the physician has the necessary information to diagnose or treat you. In addition, we may disclose your protected health information from time-to-time to another physician or health care provider (*e.g.*, a specialist or laboratory) who, at the request of your physician, becomes involved in your care by providing assistance with your health care diagnosis or treatment to your physician.

Payment: Your protected health information will be used and disclosed, as needed, to obtain payment for your health care services provided by us or by another provider. This may include certain activities that your health insurance plan may undertake before it approves or pays for the health care services we recommend for you such as: making a determination of eligibility or coverage for insurance benefits, reviewing services provided to you for medical necessity, and undertaking utilization review activities. For example, obtaining approval for a hospital stay may require that your relevant protected health information be disclosed to the health plan to obtain approval for the hospital admission.

Health Care Operations: We may use or disclose, as needed, your protected health information in order to support the business activities of your physician's practice. These activities include, but are not limited to, quality assessment activities, employee review activities, training of medical students, licensing, fundraising activities, and conducting or arranging for other business activities.

We will share your protected health information with third party "business associates" that perform various activities (for example, billing or transcription services) for our practice. Whenever an

arrangement between our office and a business associate involves the use or disclosure of your protected health information, we will have a written contract that contains terms that will protect the privacy of your protected health information.

We may use or disclose your protected health information, as necessary, to provide you with information about treatment alternatives or other health-related benefits and services that may be of interest to you. You may contact our Chief Privacy Officer to request that these materials not be sent to you.

We may use or disclose your demographic information and the dates that you received treatment from your physician, as necessary, in order to contact you for fundraising activities supported by our office. If you do not want to receive these materials, please contact our Chief Privacy Officer and request that these fundraising materials not be sent to you.

B. Disclosure:

We may use or disclose your protected health information in the following situations without your authorization or providing you the opportunity to agree or object. These situations include:

Required By Law: We may use or disclose your protected health information to the extent that the use or disclosure is required by law. The use or disclosure will be made in compliance with the law and will be limited to the relevant requirements of the law. You will be notified, if required by law, of any such uses or disclosures.

Public Health: We may disclose your protected health information for public health activities and purposes to a public health authority that is permitted by law to collect or receive the information. For example, a disclosure may be made for the purpose of preventing or controlling disease, injury or disability.

Communicable Diseases: We may disclose your protected health information, if authorized by law, to a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading the disease or condition.

Health Oversight: We may disclose protected health information to a health oversight agency for activities authorized by law, such as audits, investigations, and inspections. Oversight agencies seeking this information include government agencies that oversee the health care system, government benefit programs, other government regulatory programs and civil rights laws.

Abuse or Neglect: We may disclose your protected health information to a public health authority that is authorized by law to receive reports of child abuse or neglect. In addition, we may

disclose your protected health information if we believe that you have been a victim of abuse, neglect or domestic violence to the governmental entity or agency authorized to receive such information. In this case, the disclosure will be made consistent with the requirements of applicable federal and state laws.

Food and Drug Administration: We may disclose your protected health information to a person or company required by the Food and Drug Administration for the purpose of quality, safety, or effectiveness of FDA-regulated products or activities including, to report adverse events, product defects or problems, biologic product deviations, to track products; to enable product recalls; to make repairs or replacements, or to conduct post marketing surveillance, as required.

Legal Proceedings: We may disclose protected health information in the course of any judicial or administrative proceeding, in response to an order of a court or administrative tribunal (to the extent such disclosure is expressly authorized), or in certain conditions in response to a subpoena, discovery request or other lawful process.

Law Enforcement: We may also disclose protected health information, so long as applicable legal requirements are met, for law enforcement purposes. These law enforcement purposes include (1) legal processes and otherwise required by law, (2) limited information requests for identification and location purposes, (3) pertaining to victims of a crime, (4) suspicion that death has occurred as a result of criminal conduct, (5) in the event that a crime occurs on the premises of our practice, and (6) medical emergency (not on our practice's premises) and it is likely that a crime has occurred.

Coroners, Funeral Directors, and Organ Donation: We may disclose protected health information to a coroner or medical examiner for identification purposes, determining cause of death or for the coroner or medical examiner to perform other duties authorized by law. We may also disclose protected health information to a funeral director, as authorized by law, in order to permit the funeral director to carry out their duties. We may disclose such information in reasonable anticipation of death. Protected health information may be used and disclosed for cadaveric organ, eye or tissue donation purposes.

Research: We may disclose your protected health information to researchers when their research has been approved by an institutional review board that has reviewed the research proposal and established protocols to ensure the privacy of your protected health information.

Criminal Activity: Consistent with applicable federal and state laws, we may disclose your protected health information, if we believe that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public. We may also disclose protected health information if it is necessary for law enforcement authorities to identify or apprehend an individual.

Military Activity and National Security: When the appropriate conditions apply, we may use or disclose protected health information of individuals who are Armed Forces personnel (1) for activities deemed necessary by appropriate military command authorities; (2) for the purpose of a determination by the Department of Veterans Affairs of your eligibility for benefits, or (3) to foreign military authority if you are a member of that foreign military services. We may also disclose your protected health information to authorized federal officials for conducting national security and intelligence activities, including for the provision of protective services to the President or others legally authorized.

Workers' Compensation: We may disclose your protected health information as authorized to comply with workers' compensation laws and other similar legally-established programs.

Inmates: We may use or disclose your protected health information if you are an inmate of a correctional facility and your physician created or received your protected health information in the course of providing care to you.

C. Retention:

We shall retain your protected health information for only that period of time that is reasonable and necessary to complete the Purpose stated above in Section 1. While we are in possession of your protected health information it will be secured using the technical safeguards as outlined in the Privacy and Security Requirements of HIPAA and HITECH Act. When eHealth Technologies has concluded the Use and Disclosure consistent with the Purpose, your personal and/or protected health information will be destroyed and disposed of securely and consistent with the applicable Privacy and Security Requirements of HIPAA and HITECH Act.

5. Other Permitted and Required Uses and Disclosures That Require Providing You the Opportunity to Agree or Object

We may use and disclose your protected health information in the following instances. You have the opportunity to agree or object to the use or disclosure of all or part of your protected health information. If you are not present or able to agree or object to the use or disclosure of the protected health information, then your physician may, using professional judgment, determine whether the disclosure is in your best interest.

Facility Directories: Unless you object, we will use and disclose in our facility directory your name, the location at which you are receiving care, your general condition (such as fair or stable), and your religious affiliation. All of this information, except religious affiliation, will be disclosed to people that ask for you by name. Your religious affiliation will be only given to a member of the clergy, such as a priest or rabbi.

Others Involved in Your Health Care or Payment for your Care: Unless you object, we may disclose to a member of your family, a relative, a close friend or any other person you identify, your protected health information that directly relates to that person's involvement in your health care. If you are unable to agree or object to such a disclosure, we may disclose such information as necessary if we determine that it is in your best interest based on our professional judgment. We may use or disclose protected health information to notify or assist in notifying a family member, personal representative or any other person that is responsible for your care of your location, general condition or death. Finally, we may use or disclose your protected health information to an authorized public or private entity to assist in disaster relief efforts and to coordinate uses and disclosures to family or other individuals involved in your health care.

6. Securing your Personal and/or Protected Health Information

eHealth Technologies has a robust Privacy and Security Program that includes, but not limited too; risk, policy, organizational security, asset management, human resource security, Privacy Officer, Security Officer, Security Engineer, physical and environmental security, secure communications and operations, access controls, information systems maintenance, security incident management, business continuity and compliance.

7. Quality

eHealth Technologies ensures quality with regards to the personal and protected data obtained through consent or otherwise permitted or required by law as described herein, and that it is complete and accurate for the purposes for which it is to be used. Individuals are informed, at the time of collection and thereafter, that they are responsible for providing accurate and complete personal information, and must contact eHealth Technologies if a correction is required.

8. Your Rights

Following is a statement of your rights with respect to your personal or protected health information and if necessary a brief description of how you may exercise these rights.

a. **You have the right to know the purpose for which your personal and/or protected health information is being collected and is stated as such in this notice.**

b. **You have the right to choose when your personal and/or protected health information is being collected, unless a law or regulation specifically requires or allows otherwise and is stated as such in this notice.**

c. **You have the right to know how your personal and/or protected health information is being collected and is stated as such in this notice.**

d. **You have the right to know how your personal and/or protected health information is being used, how long it is being retained, and how it is disposed of and is stated as such in this notice.**

e. **You have the right to access your personal and/or protected health information and as stated as such in this notice.**

f. **You have the right to have your personal and/or protected health information secured and as stated as such in this notice.**

g. **You have the right to ensure your personal and/or protected health information is accurate and complete.**

h. **You have the right to inspect and copy your personal and/or protected health protected health information.** This means you may inspect and obtain a copy of protected health information about you for so long as we maintain the protected health information. You may obtain your medical record that contains medical and billing records and any other records that your physician and the practice uses for making decisions about you. As permitted by federal or state law, we may charge you a reasonable copy fee for a copy of your records.

   Under federal law, however, you may not inspect or copy the following records: psychotherapy notes; information compiled in reasonable anticipation of, or use in, a civil, criminal, or administrative action or proceeding; and laboratory results that are subject to law that prohibits access to protected health information. Depending on the circumstances, a decision to deny access may be reviewable. In some circumstances, you may have a right to have this decision reviewed. Please contact our Chief Privacy Officer if you have questions about access to your medical record.

i. **You have the right to request a restriction of your personal and/or protected health information.** This means you may ask us not to use or disclose any part of your protected health information for the purposes of treatment, payment or health care operations. You may also request that any part of your protected health information not be disclosed to family members or friends who may be involved in your care or for notification purposes as described in this Notice of Privacy Practices. Your request must state the specific restriction requested and to whom you want the restriction to apply.

Your physician is not required to agree to a restriction that you may request. If your physician does agree to the requested restriction, we may not use or disclose your protected health information in violation of that restriction unless it is needed to provide emergency treatment. With this in mind, please discuss any restriction you wish to request with your physician. You may request a restriction by submitting written notice of the specific restrictions including all names, addresses, and specifically restricted information to our Chief Privacy Officer.

j. **You have the right to request to receive confidential communications from us by alternative means or at an alternative location.** We will accommodate reasonable requests. We may also condition this accommodation by asking you for information as to how payment will be handled or specification of an alternative address or other method of contact. We will not request an explanation from you as to the basis for the request. Please make this request in writing to our Chief Privacy Officer.

k. **You may have the right to have your physician amend your protected health information.** This means you may request an amendment of protected health information about you in a designated record set for so long as we maintain this information. In certain cases, we may deny your request for an amendment. If we deny your request for amendment, you have the right to file a statement of disagreement with us and we may prepare a rebuttal to your statement and will provide you with a copy of any such rebuttal. Please contact our Chief Privacy Officer if you have questions about amending your medical record.

l. **You have the right to receive an accounting of certain disclosures we have made, if any, of your personal and/protected 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. It excludes disclosures we may have made to you if you authorized us to make the disclosure, for a facility directory, to family members or friends involved in your care, or for notification purposes, for national security or intelligence, to law enforcement (as provided in the privacy rule) or correctional facilities, as part of a limited data set disclosure. You have the right to receive specific information regarding these disclosures that occur after April 14, 2003. The right to receive this information is subject to certain exceptions, restrictions and limitations.

m. **You have the right to obtain a paper copy of this notice from eHealth Technologies**, **upon request, even if you have agreed to accept this notice electronically**.

9. Complaints

If you believe your privacy rights have been violated by eHealth Technologies, you may file a compliant by notifying our Chief Privacy Officer or to the Secretary of Health and Human Services.

You may contact our Chief Privacy Officer, Michael A. Sciortino, Esq., at (877) 344-8999 or by email at michael.sciortino@ehealthtechnologies.com for further information about the complaint process. All written notices and communication must be sent directly to our Chief Privacy Officer, Michael A. Sciortino, Esq., eHealth Global Technologies, Inc. d/b/a eHealth Technologies, 250 Thruway Park Drive, West Henrietta, New York 14586.

This Notice of Privacy Practices is published electronically and available in writing upon request. This notice is subject to change at anytime and all updates will be posted on the website accordingly.