eHEALTH GLOBAL TECHNOLOGIES, INC.
d/b/a
eHEALTH TECHNOLOGIES

250 Thruway Park Drive
West Henrietta, New York 14586

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 Notice of Privacy Practices, or the Privacy and Security of any Health Information, please contact our Compliance Department and contact 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 personal and/or 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 collecting and disclosure of medical records and images, 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 personal and/or protected health information. "Protected health information" is information about you, including demographic information and other identifiers including but not limited to name, address, date of birth, phone numbers, email addresses, social security numbers, Medical Record Numbers, and Health Plan Beneficiary Numbers, that may identify you and that relates to your past, present or future physical or mental health 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 personal and/or 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 personal and/or protected health information while it is in our control and custody. This Notice of Privacy Practices does not govern the independent hospitals, medical practices, or other 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 is contracted by Covered Entities to collect and disclose your personal and/or protected health information to that Covered Entity or other health care provider for their continued treatment of you, for payment, or for 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 the collection and disclosure of information to a Covered Entity including a requestor of medical records or a provider of medical records, 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 approval and signature, 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 in all other circumstances, 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 a 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, Access, and Retention of Protected Health Information

A. Use and Access:

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 Covered Entities and Business Associates are permitted to make. These examples are not meant to be exhaustive or directly applicable to eHealth Technologies, but to describe the types of uses and disclosures that may be made by Covered Entities and Business Associates:

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. If applicable, these activities may 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 may also be required to deliver your protected health information to third party subcontractors, or "business associates" of eHealth Technologies that perform various activities (for example, data center security services or transcription services) for our office. 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 known as a Business Associate Agreement that contains terms that will protect the privacy of your personal and/or protected health information.

B. Disclosure:

We may use or disclose your personal and/or 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 personal and/or 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 personal and/or 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 personal and/or 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 personal and/or 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 personal and/or 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 personal and/or 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 personal and/or protected health information to a person or company required by the Food and Drug Administration ("FDA") 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 personal and/or 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 personal and/or 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 our premises, and (6) medical emergency (not on our premises) and it is likely that a crime has occurred.

Coroners, Funeral Directors, and Organ Donation: We may disclose personal and/or 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 personal and/or 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. Personal and/or protected health information may be used and disclosed for cadaveric organ, eye or tissue donation purposes.

Research: We may disclose your personal and/or 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 personal and/or protected health information.

Criminal Activity: Consistent with applicable federal and state laws, we may disclose your personal and/or 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 personal and/or 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 personal and/or 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 personal and/or protected health information to authorized federal officials for conducting national security and intelligence activities, including for the provision of protective services to the President of the United States of America, or others legally authorized.

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

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

C. Retention:

We shall retain your personal and/or 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 personal and/or protected health information it will be secured using the administrative, physical, and 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, including shredding, wiping, erasing, or destruction of data.

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

eHealth Technologies does wish to advise you that although unlikely, we may use and disclose your personal and/or protected health information in the following instances where you have the absolute right to agree or to object to the use or disclosure of all or part of your personal and/or protected health information in this manner:

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 personal and/or 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 personal and/or 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 personal and/or 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 assessments and breach notification policies, policy development and review, 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. Through this Privacy and Security Program, eHealth Technologies is able to provide significant protection for very sensitive and confidential information including your personal and/or protected health information.

7. Quality

eHealth Technologies ensures quality with regards to the personal and protected data obtained through your consent and/or written authorization, or otherwise permitted or required by law through continuity of care provisions 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 and/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 of Privacy Practices.

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 of Privacy Practices.**

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 of Privacy Practices.**

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 of Privacy Practices.**

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

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

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 personal and/or protected health information prior to its destruction. 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. Please contact our Chief Privacy Officer if you have questions about access to your personal and/or protected health information.

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 personal and/or protected health information for the purposes of treatment, payment or health care operations. You may also request that any part of your personal and/or protected health information not be disclosed to family members or friends who may be involved in your care or for notification purposes as described above in this Notice of Privacy Practices. Your request must state the specific restriction requested and to whom you want the restriction to apply. 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 and 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. We may condition this accommodation by asking you for information or specification of an alternative address or other method of contact.

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 and direct said request to your physician or treating hospital. In certain cases, we may deny your request for an amendment as eHealth Technologies is not a treating medical provider but rather a Business Associate and does not have the authority to make any said amendments. To the extent applicable, we may provide you with the contact information of your physician or treating hospital to make your request for an amendment. 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, 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. Privacy and Security of Health Information

eHealth Technologies is committed to preserving the security and privacy of all patient data and information. eHealth Technologies' Compliance Officer is its internal Chief General Counsel and Chief Privacy Officer, Michael A. Sciortino, Esq. who may be reached directly at (585) 242-1019. Along with an Information Security Officer, eHealth Technologies closely monitors the security

and privacy of all health information to ensure the HIPAA requirements are met. If you have a concern about the privacy and security of any health information, you may reach our Compliance Officer by contacting our Chief Privacy Officer, Michael A. Sciortino, Esq., directly at (585) 242-1019, or toll free at (877) 344-8999, or by email at michael.sciortino@ehealthtechnologies.com for further information. Written communication may be directed to 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.

10. Complaints

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

You may contact our Compliance Department through Chief Privacy Officer, Michael A. Sciortino, Esq., directly at (585) 242-1019, or toll free 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 of Privacy Practices is subject to change at anytime and all updates will be posted on the website accordingly.