BENEFITS ADMINISTRATION AND WELLNESS

Privacy Statement

OMNIBUS Rule

HIPAA NOTICE OF PRIVACY PRACTICES

Ebix Inc.

Address: Ebix, Inc.

1 Ebix Way

Johns Creek, GA 30097

THIS NOTICE DESCRIBES HOW PROTECTED HEALTH INFORMATION (PHI) ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION under the HIPAA Omnibus Rule of 2013.

PLEASE REVIEW IT CAREFULLY

For purposes of this Notice, “us” “we” and “our” refers to the Name of this company, Ebix, Inc., and “you” or “your” refers to our participants (or their legal representatives as determined by us in accordance with state informed consent law). When you receive health and wellness services from us, we may obtain access to your PHI (for example, your biometric screening results). We are committed to maintaining the privacy of your PHI and we have implemented numerous procedures to ensure that we do so.

The Federal Health Insurance Portability & Accountability Act of 2013, HIPAA Omnibus Rule, (formally HIPAA 1996 & HI TECH of 2004) require us to maintain the confidentiality of all your healthcare records and other identifiable protected health information (PHI) used by or disclosed to us in any form, whether electronic, on paper, or spoken. HIPAA is a Federal Law that gives you significant new rights to understand and control how your health information is used. Federal HIPAA Omnibus Rule and state law provide penalties for covered entities, business associates, and their subcontractors and records owners, respectively that misuse or improperly disclose PHI.

Starting April 14, 2003, HIPAA requires us to provide you with the Notice of our legal duties and the privacy practices we are required to follow. If you have any questions about this Notice, please ask to speak to our HIPAA Privacy Officer.

Our doctors, clinical staff, employees, Business Associates (outside contractors we hire), their subcontractors and other involved parties follow the policies and procedures set forth in this Notice.

This notice takes effect September 23, 2013. We reserve the right to change the terms of this notice at any time and make any new provisions effective as to all PHI we maintain about you, including PHI we created or received before we made the changes.

We will notify you of any substantial changes to this notice within [60] days of the change.

The Information We Routinely Collect.

We may collect information directly from you through your participation in our programs and services on this site, as well as from other organizations such as biometric screening companies, health coaching vendors, your employer, or health insurance companies that participate in your wellness program. Typical information includes, but is not limited to: demographic information (such as your name, email address, and occupation), biometric information from health screening activities, program eligibility information and participation information.

If you receive e-mail updates, news, announcements and/or special notices from Ebix's beBetter Health application, Ebix's beBetter Health application uses the name, demographic, e-mail and other contact information you supply to provide those updates, news, announcements and notices through its own facilities or those of a contracted service supplier. Your e-mail address and other contact information will be used only for program-related mailings and will not be given, sold or rented to any other party for any other use without your prior approval.

How We Use Information About You.

We may use information about you to notify you of opportunities available on or through the Site, to customize the Site content for you, to send you materials that you request from us, and for other legitimate and lawful business purposes.

Ebix may combine information about you with information about others who use the Site and remove all personal identifiers from the resulting combined information to create "de-identified information." We use de-identified information in the development of products and services to meet the continuing needs of our clients, and to analyze and improve the content, features, materials, and opportunities that we may make available on the Site.

In addition, data or information may be used to determine qualifying for various program incentives, evaluating and reporting program results. Information of this nature may be shared with sponsoring organizations for purposes of benefit payment or various accounting functions.

If you contact us for support or assistance, we may use information about you or your computer that you provide for purposes such as verifying whether your computer meets the minimum requirements needed to use the Site and our various services.

Data collected by our Web servers or otherwise through use of the Site is used to facilitate Site operation and system administration, to generate aggregated, non-identifiable statistical information, to monitor and analyze Site traffic and usage patterns, and to improve the content and content delivery with regard

to the Site and the content, materials, opportunities, and services that we describe or make available on the Site. These data may reveal such things as the Internet Protocol address assigned to your computer, specific pages that you accessed on the Site or immediately prior to visiting the Site, and the length of time you spend at the Site, but without combining these data with other sources of information, they do not readily or personally identify you. For security reasons and to confirm the integrity of our data, however, we may combine components of these data with other sources of information that may identify you. Unless otherwise described in this Notice of Privacy Practices, such information will be used solely for our internal business purposes.

OUR RULES ON HOW WE MAY USE AND DISCLOSE YOUR PROTECTED HEALTH INFORMATION

By accessing and using the Site, you agree that you have read and understand this Notice of Privacy Practices and that you accept and consent to the privacy practices (and any uses and disclosures of information about you) that are described in this Notice of Privacy Practices.

Documentation – You will be asked to accept a Notice of Privacy Practices. If you did not accept this Notice or need a copy of the one you accepted, please contact our Privacy Officer. You may take back or revoke your consent or authorization at any time (unless we already have acted based on it) by submitting our Revocation Form in writing to us at our address listed herein. Your revocation will take effect when we actually receive it. We cannot give it retroactive effect, so it will not affect any use or disclosure that occurred in our reliance on your Consent or Authorization prior to revocation.

Special Rules

Notwithstanding anything else contained in this Notice, only in accordance with applicable HIPAA Omnibus Rule, and under strictly limited circumstances, we may use or disclose your PHI without your permission, consent or authorization for the following purposes:

- When required under federal, state or local law
- When necessary in emergencies to prevent a serious threat to your health and safety or the health and safety of other persons
- When necessary for public health reasons (for example, prevention or control of disease, injury or disability, reporting information such as adverse reactions to anesthesia, ineffective or dangerous medications or products, suspected abuse, neglect or exploitation of children, disabled adults or the elderly, or domestic violence)
- For federal or state government healthcare oversight activities (for example., civil rights laws, fraud and abuse investigations, audits, investigations, inspections, licensure or permitting, government programs.)
- For judicial and administrative proceedings and law enforcement purposes (for example, in response to a warrant, subpoena or court order, by providing PHI to coroners, medical examiners and funeral directors to locate missing persons, identify deceased persons or determine cause of death)
- For Worker's Compensation purposes (i.e., we may disclose your PHI if you have claimed health benefits for a work-related injury or illness)

- For intelligence, counterintelligence or other national security purposes (i.e., Veterans Affairs, U.S. military command, other government authorities or foreign military authorities may require us to release PHI about you)

- For organ and tissue donation (i.e., if you are an organ donor, we may release your PHI to organizations that handle organ, eye or tissue procurement, donation and transplantation)

- For research projects approved by an Institutional Review Board or a privacy board to ensure confidentiality (i.e., if the researcher will have access to your PHI because involved in your clinical care, we will ask you to sign an authorization)

- To create a collection of information that is "de-identified" (i.e., it does not personally identify you by name, distinguishing marks or otherwise and no longer can be connected to you)

- To family members, friends and others, but only if you are present and verbally give permission. We give you an opportunity to object and if you do not, we reasonably assume, based on our professional judgment and the surrounding circumstances, that you do not object (i.e.. you bring someone with you into an exam room during treatment or into the conference area when we are discussing your PHI); we reasonably infer that it is in your best interest (i.e., to allow someone to pick up your records because they knew you were our patient and you asked them in writing with your signature to do so); or it is an emergency situation involving you or another person (i.e., your minor child or ward) and, respectively, you cannot consent to your care because you are incapable of doing so or you cannot consent to the other person's care because, after a reasonable attempt, we have been unable to locate you. In these emergency situations we may, based on our professional judgment and the surrounding circumstances, determine that disclosure is in the best interests of you or the other person, in which case we will disclose PHI, but only as it pertains to the care being provided and we will notify you of the disclosure as soon as possible after the care is completed.

Minimum Necessary Rule

Our staff will not use or access your PHI unless it is necessary to do their jobs (i.e., doctors uninvolved in your care will not access your PHI; ancillary clinical staff caring for you will not access your billing information; billing staff will not access your PHI except as needed to complete the claim form for the latest visit; janitorial staff will not access your PHI). All of our team members are trained in HIPAA Privacy rules and sign strict Confidentiality Contracts with regards to protecting and keeping private your PHI. So do our Business Associates and their

Subcontractors. Know that your PHI is protected several layers deep with regards to our business relations. Also, we disclose to others outside our staff, only as much of your PHI as is necessary to accomplish the recipient's lawful purposes. Still in certain cases, we may use and disclose the entire contents of your medical record:

- To you (and your legal representatives as stated above) and anyone else you list on a Consent or Authorization to receive a copy of your records

- To healthcare providers for treatment purposes (i.e., making diagnosis and treatment decisions or agreeing with prior recommendations in the medical record)

- To the U.S. Department of Health and Human Services (i.e., in connection with a HIPAA complaint)

- To others as required under federal or state law

- To our Privacy Officer and others as necessary to resolve your complaint or accomplish your request under HIPAA (for example, clerks who copy records need access to your entire medical record)

In accordance with HIPAA law, we presume that requests for disclosure of PHI from another Covered Entity (as defined in HIPAA) are for the minimum necessary amount of PHI to accomplish the requestor's purpose. Our Privacy Officer will individually review unusual or non-recurring requests for PHI to determine the minimum necessary amount of PHI and disclose only that. For non-routine requests or disclosures, our Privacy Officer will make a minimum necessary determination based on, but not limited to, the following factors:

- The amount of information being disclosed

- The number of individuals or entities to whom the information is being disclosed

- The importance of the use or disclosure

- The likelihood of further disclosure

- Whether the same result could be achieved with de-identified information

- The technology available to protect confidentiality of the information

- The cost to implement administrative, technical and security procedures to protect confidentiality

Incidental Disclosure Rule

We will take reasonable administrative, technical and security safeguards to ensure the privacy of your PHI when we use or disclose it (i.e., we shred all paper containing PHI, require employees to speak with privacy precautions when discussing PHI with you, we use computer passwords and change them periodically (i.e., when an employee leaves us), we use firewall and router protection to the federal standard, we back up our PHI data off-site and encrypted to federal standard, we do not allow unauthorized access to areas where PHI is stored or filed and/or we have any unsupervised business associates sign Business Associate Confidentiality Agreements).

However, in the event that there is a breach in protecting your PHI, we will follow Federal Guide Lines to HIPAA Omnibus Rule Standard to first evaluate the breach situation using the Omnibus Rule, 4-Factor Formula for Breach Assessment. Then we will document the situation, retain copies of the situation on file, and report all breaches (other than low probability as prescribed by the Omnibus Rule) to the US Department of Health and Human Services at:

https://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html

We will also make proper notification to you and any other parties of significance as required by HIPAA Law.

Business Associate Rule

Business Associates are defined as: an entity, (non-employee) that in the course of their work will directly/indirectly use, transmit, view, transport, hear, interpret, process or offer PHI for this Facility.

Business Associates and other third parties (if any) that receive your PHI from us will be prohibited from re-disclosing it unless required to do so by law or you give prior express written consent to the re-disclosure. Nothing in our Business Associate agreement will allow our Business Associate to violate this re-disclosure prohibition. Under Omnibus Rule, Business Associates will sign a strict confidentiality agreement binding them to keep your PHI protected and report any compromise of such information to us, you and the United States Department of Health and Human Services, as well as other required entities. Our Business Associates will also follow Omnibus Rule and have any of their Subcontractors that may directly or indirectly have contact with your PHI, sign Confidentiality Agreements to Federal Omnibus Standard.

Security Practices

We use commercially reasonable methods to keep information about you that we collect or store on or through the Site safe from unauthorized access. Because Ebix respects your privacy and values your trust, the only persons to whom we give access to information about you are those who use it to provide services to you or conduct other activities described in this Notice of Privacy Practices. Ebix maintains physical, electronic, and procedural safeguards designed to comply with applicable federal standards to help guard information about you and to assist us in preventing unauthorized access to that information. Nevertheless, no set of security safeguards is guaranteed to be impenetrable. We cannot and do not guarantee that communications to or from the Site, or that data transmitted or stored on or through the Site, are or will be totally secure from loss, misuse or unauthorized access by third parties.

Your Rights:

You have the following rights regarding your PHI:

Restriction. Request that we place additional restrictions on our use or disclosure of your PHI, but we are not obligated to agree to any such additional restrictions. Any such agreement by us must be in writing signed by a person authorized to make such an agreement on our behalf. We will not be bound unless our agreement is in writing.

Confidential Communication. Request that you receive communications of PHI by alternative means or at alternative locations. You must make your request in writing. This right only applies if the information could endanger you if it is not communicated by the alternative means or to the alternative location you want. You do not have to explain the basis for your request, but you must clearly state that the information could endanger you if the communication means or location is not changed. We must accommodate your request if it is reasonable, specifies the alternative means or location, and provides satisfactory explanation how payments will be handled under the alternative means or location you request.

Access. Subject to limited exceptions, access, inspect and obtain a copy of PHI we maintain about you in a designated record set. A "designated record set" contains records we maintain such as enrollment, claims processing, and case management records. All such requests must be in writing and sent to the contact person provided in this Notice. You may request the information in electronic format and may direct that it be sent to another designated person or entity.

Amendment. With limited exceptions, request that we amend your PHI that we maintain in a designated record set. Your request must be in writing, and it must explain why the information should be amended. We may deny your request if we did not create the information you want amended and the originator remains available or for certain other reasons.

Notice. Receive notice from us if any of your unsecured PHI has been compromised ("breach") within a reasonable time but no longer than 60 days following discovery of the breach.

Notice to California Residents under CCPA Regulation:

What are your rights?

You have a number of rights in relation to your personal data which should be exercised by contacting the User or 'controller' of this data. As a service provider Ebix may only be a 'custodian' of the data holding it on behalf of the 'controller'. You have the right to request the 'controller' provide access to various details about data usage. This may include data access, data history, data retention requests for the erasure of data no longer required, requests to restrict access on the processing or usage of your data,

Contact and complaints

You can contact us with any queries or concerns at the following email address Privacy@ebix.com

If you have a complaint or concern about how we use your personal data, please contact us in the first instance and we will attempt to resolve the issue as soon as possible. In the US, the supervisory authority for data protect ion is the I COOAG (https://oag.ca.gov/privacy/ccpa). We do ask that you please attempt to resolve any issues with us first, although you have a right to contact your supervisory authority at any time.

Further information on CCPA regulation can be found at https://oag.ca.gov/privacy/ccpa

To Complain or Get More Information

We will follow our rules as set forth in this Notice. If you want more information or if you believe your privacy rights have been violated (i.e., you disagree with a decision of ours about inspection / copying, amendment / correction, accounting of disclosures, restrictions or alternative communications), we want to make it right. We never will penalize you for filing a complaint. To do so, please file a formal, written complaint within 180 days with:

The U.S. Department of Health & Human Services

Office of Civil Rights

200 Independence Ave., S.W.

Washington, DC 20201

877.696.6775

If you have any questions regarding this Privacy Notice of Privacy Practices, please write Ebix at:

HIPAA Privacy Officer

Ebix, Inc.

1 Ebix Way

Johns Creek, GA 30097

You may get your “**HIPAA Complaint”** form by contacting our Privacy Officer.

These privacy practices are in accordance with the original HIPAA enforcement effective April 14, 2003, and undated to Omnibus Rule effective March 26, 2013 and will remain in effect until we replace them as specified by Federal and/or State Law.

©Ebix, Inc. 2024