NOTICE OF PRIVACY PRACTICES
FOR THE BJC PLANS

Original Effective Date: April 14, 2003
Revised: 1/1/04, 1/1/05, 8/30/06, 1/1/08, 9/1/09, 9/1/10, 9/20/11, 09/23/13, 9/23/14
Last Revision Date: August 28, 2015

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.

The Health Insurance Portability and Accountability Act of 1996 and the regulations thereunder (“HIPAA”) require a health plan to notify participants about its privacy policies and procedures with respect to participants’ health information. This document is intended to satisfy HIPAA’s notice requirement.

This document serves as the required Notice for the health plans sponsored by BJC Health System (“BJC”). The health plans covered by this Notice include the following: BJC HealthCare Medical and Dental Plan, BJC HealthCare Access Plus Plan, BJC HealthCare Vision Plan, Health Care Reimbursement Account Program, and BJC HealthCare Employee Assistance Program (“EAP Program”). The plans and programs listed in the immediately preceding sentence are component programs of the BJC HealthCare Health and Welfare Plan (PN 515). This Notice only applies to the component programs listed above which are collectively referred to herein as the “Plans”.

The Plans have authorized certain BJC employees to have access to your health information so that they may perform certain administrative functions for the Plans. These administrative functions—treatment, payment, and health care operations—are described below. These authorized employees also may use and disclose your health information for other purposes, which are outlined in this Notice. Note, however, that only the Privacy Officer (or a designee), the Security Officer (or a designee), the Vice President of Corporate Compliance (or a designee), the Privacy Liaison of the Plans, and those employees in the BJC Health System Legal Services Department responsible for the EAP Program may have access to health information with respect to the EAP Program, and that access is strictly limited to the information necessary to carry out the management duties relating to implementation of and compliance with the requirements of the HIPAA and the HIPAA privacy and security regulations; no other BJC employees have been authorized to have access to your EAP health information for any purpose.

The Plans may share enrollment information with BJC, and may provide summary health information to BJC for Plan design purposes.

This Notice will describe the ways in which BJC employees with access to your protected health information and the Plans’ third party administrators (“TPAs”) and other business associates may use and disclose such information. This Notice also describes the Plans’ obligations and your rights regarding the use and disclosure of your health information.

The Plans’ business associates are subject to the HIPAA privacy and security rules in the same way that the Plan is subject to such rules. In addition, each of the Plans’ business associates is required to enter into a business associate agreement with the Plan to safeguard your health information in accordance with HIPAA.

This Notice also describes the Plans’ obligations and your rights regarding the use and disclosure of your health information.

If you have a benefits question or issue that involves your protected health information, you should contact the BJC Benefits Department to speak to the appropriate authorized employee. You should not
share your or your dependents’ protected health information with your local Human Resources (HR) office. Local HR offices are not authorized personnel with access to use or disclose your protected health information. Local HR offices are able to discuss limited issues relating to general eligibility and enrollment and general benefits under the Plans.

References to “we” or “our” throughout this Notice refer to the Plans and the BJC employees who are authorized to access your health information for administration of the Plans.

Our Commitment to Your Privacy

We respect the confidentiality of your health information and recognize that information about your health is personal. This Notice informs you of your rights regarding the privacy of your protected health information and how we may use and disclose such information. In this Notice, we refer to our uses and disclosures of protected health information as our “Privacy Practices.” Protected health information generally includes information that we create or receive that identifies you and your past, present or future health status, the provision of care, or the payment for that care.

The Plans are required by HIPAA to:

• make sure that your health information is kept private;
• give you this Notice of our Privacy Practices and legal duties with respect to your protected health information; and
• follow the terms of the Notice currently in effect.

In addition, if a Plan determines that a breach (as defined by law) of your unsecured protected health information has occurred, the Plan must notify you of the breach. The Plan must also notify the Department of Health and Human Services, and in some cases, may be required to provide some general notification to the media.

What Types of Personal Information Do We Collect?

To administer your benefits, we need information about you. We collect enrollment data and other information. This information may come from you, your employer, other health benefit plans, or other administrators for the Plans. Examples of information that may be obtained include your name, address, phone number, social security number, date of birth, marital status, employment information, or medical history. We also receive information from health care providers and others about you, such as the health care services you receive. This information may be in the form of health care claims and encounters, medical information or a service request. We may receive your information in writing, by telephone or electronically.

How Do We Protect the Privacy of Your Personal Information?

We limit access to your protected health information to only those who need it and we maintain appropriate safeguards to protect it. For example, we protect access to our buildings and computer systems. We provide training to authorized employees regarding protecting the privacy of your personal information.

How Do We Use and Disclose Your Information for Treatment, Payment and Health Care Operations?

The following categories describe different ways in which we and our business associates may use and disclose your protected health information. Not every use or disclosure in a category will be listed. In any event, the Plans are prohibited from using or disclosing any genetic protected health information for underwriting purposes and from communications with you without your authorization concerning a product or service when the Plan receives remuneration for making the communication from the third party whose product or service is being marketed.
**Treatment:** We and our business associates may use and disclose your health information with health care providers for coordination and management of your care. Providers include physicians, hospitals and other caregivers who provide services to you.

**Payment:** We and our business associates may use and disclose your health information to make coverage determinations and payment in accordance with the terms of the Plan (this includes billing, claims management, subrogation, reviews for medical necessity and appropriateness of care, utilization review and preauthorization). For example, a business associate may tell your health care provider whether you are eligible for Plan coverage. In addition, your health information may be shared with another health plan to coordinate benefit payments. Also, certain employees of the BJC Benefits Department will have access to your health information that is relevant to an appeal you file under the Plan.

**Health Care Operations:** We and our business associates may use and disclose your health information as part of the Plans’ operations. Operations includes quality assessment and improvement activities; grievance or external review programs; disease management, case management and care coordination; and health and wellness programs. This also may include general administrative activities such as detection and investigation of fraud; auditing; underwriting and ratemaking; or securing and servicing reinsurance policies. For example, we may use or disclose your health information to evaluate the quality of health care delivered, to remind you about preventive care or to inform you about a disease management program. Our TPAs and business associates may use or disclose your personal information with each other to facilitate health and wellness programs for plan participants and covered dependents. In addition, we and our business associates may contact you to provide you information about treatment alternatives or other health-related benefits that may be of interest to you.

**What Other Ways Do We Use or Disclose Your Information?**

We also may use or disclose your protected health information for the following:

**Legal requirements.** The Plan may be required by law to disclose your health information.

**HIPAA enforcement.** The Plan will make your health information available to you, and to the Secretary of the Department of Health and Human Services for purposes of HIPAA enforcement.

**Public health agencies and governmental authority.** Your health information may be disclosed to a public health agency. This may include disclosing your health information to report certain diseases, death, abuse, neglect or domestic violence or reporting information to the Food and Drug Administration, if you experience an adverse reaction from any of the drugs, supplies or equipment that are involved in your care.

**Health care oversight and law enforcement.** Your health information may be disclosed to government agencies so they can monitor, investigate, inspect, discipline or license those who work in the health care system or for government benefit programs.

**Workers’ compensation laws.** Your health information may be disclosed as authorized by law to comply with workers’ compensation laws.

**Legal proceedings.** Your health information may be disclosed in the course of a judicial or administrative proceeding, in response to an order of a court or administrative tribunal (to the extent such disclosure is expressly authorized); and in response to a subpoena, discovery request, or other lawful process, provided certain conditions are met.

**Crime.** Your health information may be disclosed to law enforcement officials to report or prevent a crime, locate or identify a suspect, fugitive or material witness or assist a victim of a crime.

**Threat to health or safety.** Your health information may be used or disclosed to avert a serious threat to health or safety if the use or disclosure is necessary to prevent a serious and imminent threat to the health or safety of a person or to the public, and is disclosed to a person who is reasonably able to prevent or lessen the threat, including the target of the threat.

**Research.** Your health information may be used or disclosed for limited research purposes, provided that a waiver of the authorization required by HIPAA has been approved by an appropriate privacy board.
**Member of Armed Forces.** If you are a member of the armed forces, the Plan may disclose your health information as required by military command authorities or to evaluate your eligibility for veteran’s benefits. The Plan also may disclose health information about foreign military personnel to the appropriate foreign military authority.

**Coroners, medical examiners and funeral directors.** Your health information may be disclosed to coroners, medical examiners and funeral directors so that they can carry out their duties or for purposes of identification or determining cause of death.

**Cadaveric organ, eye or tissue donation.** Your health information may be disclosed to people involved with obtaining, storing or transplanting organs, eyes or tissue of cadavers for donation purposes.

**National Security.** The Plan may disclose your health information to authorized federal officials for intelligence, counterintelligence, and other national security activities authorized by law.

**Inmate.** If you are an inmate of a correctional institution or under the custody of a law enforcement official, the Plan may release your health information to the correctional institution or law enforcement official.

**Others involved in your care.** We may disclose certain health information with a relative, such as your spouse, close personal friend, or others whom we have verified are involved in your care or payment for that care. For example, we may mail explanations of benefits paid to the subscriber. Your family also may have access to such information on our web sites.

**Personal representatives.** We may disclose health information with people you have authorized or those having a relationship that gives them the right to act on your behalf. Examples include parents of an unemancipated minor or those having a Power of Attorney.

**Pursuant to an authorization.** We will obtain your written authorization to use or disclose your health information for reasons not identified by this Notice. (For example, uses and disclosures of PHI for marketing purposes, and disclosures that constitute a sale of PHI would require your authorization.) If you revoke your authorization, we will no longer use or disclose your health information for those reasons following receipt of your written revocation.

---

**What are Your Rights Established by Law?**

You have the following rights with respect to your health information. You must notify us in writing to exercise these rights.

**Requesting restrictions:** You have the right to request a restriction on the health information that the Plan(s) may use or disclose about you for treatment, payment or health care operations, or that the Plan(s) may disclose to your spouse, a family member or a close personal friend who is involved with payment related to your health care. In general, we are not required to, and generally will not, agree to your request. However, we are required to agree to a request to restrict disclosure of your protected health information for payment or health care operations (but not for treatment) if you have paid your provider in full, out-of-pocket.

Requests for restrictions must be made in writing to the Privacy Officer c/o Director, Benefits. In your request, you must provide: (1) what information you want to restrict; (2) whether you want to restrict use, disclosure or both; and (3) to whom you want the restrictions to apply.

**Confidential communications:** You have the right to request that we communicate with you in a certain way, or at a certain location. For example, you may ask that we contact you by mail, rather than by telephone, or at work, rather than at home. Requests for confidential communications must be made in writing to the Privacy Officer c/o Director, Benefits. We will attempt to honor all reasonable requests.

**Inspect and copy:** You have the right to inspect and obtain a copy of coverage, payment, claims and other health information used by the Plan(s) to make benefit determinations about you. We may deny your request to inspect or copy your health information in some situations. In some cases, you may have the right to request a review of such a decision to deny this access. We will provide you this information free of charge, unless we already provided this to you within the same 12-month period. In that case, we may charge a fee for the costs of
copying, mailing, labor and supplies related to your request. We will notify you of the costs involved with additional requests, and you may withdraw your request before you incur any costs.

Amendment: You have the right to request that the Plan(s) amend your coverage, payment and claims record and other health information used by the Plan to make benefit determinations about you. You have the right to request an amendment for as long as the information is maintained by or for the Plan. To request an amendment, you must submit your request in writing to the Privacy Officer c/o Director, Benefits. In addition, you must provide a reason that supports your request. If your request is denied in whole or in part, the Plan(s) will provide you with a written denial that explains the basis for the denial. You may then submit a written statement disagreeing with the denial and have that statement included with any future disclosure of your health information.

Accounting of disclosures: You have the right to request an “accounting” of the Plan(s)’ disclosures of your health information. Examples include sharing your information in response to court orders or with government agencies that license us. There are exceptions to the types of disclosures for which the Plans are required to account. For example, the Plans are not required to give you an accounting of disclosures of your health information for purposes of treatment, payment or health care operations. To request an accounting of disclosures, you must submit your request in writing to the Privacy Officer c/o Director, Benefits. All requests for an accounting of disclosures must state a time period that may not include a date earlier than six years prior to the date of the request and may not include dates before April 14, 2003. We will provide you with the list free of charge, unless we already provided you with a list within the same 12-month period. We will notify you of the costs involved with additional requests, and you may withdraw your request before you incur any costs.

Paper Copy of this Notice: You have the right to a paper copy of this Notice. You may ask us to give you a copy of this Notice at any time. You also may obtain a copy of this notice on the BJC intranet.

Changes to This Notice

The Plans reserve the right to change the terms of this Notice. The Plans reserve the right to make any changes to this Notice apply to all of your health information already maintained by the Plans, as well as any information that the Plans may receive or create in the future. In the event of a material change to this Notice, a revised version of this Notice will be provided to you in a manner permitted by the HIPAA privacy regulations.

Complaints

If you believe your privacy rights have been violated, you may file a complaint with the Plan(s) or with the Secretary of the U.S. Department of Health and Human Services. To file a complaint with the Plan(s), contact the Director, Benefits at the following address: Mail Stop 92-92-248, 8300 Eager Road, Suite 300C, St. Louis, Missouri 63144-1412.

All complaints must be submitted in writing. You will not be retaliated against for filing a complaint.

For Further Information

If you have any questions about this Notice, please contact the Director, Benefits at (314) 362-7582 or at the following address: Mail Stop 92-92-248, 8300 Eager Road, Suite 300C, St. Louis, Missouri 63144-1412. The Director, Benefits serves as the Privacy Liaison for the Plans covered under this Notice.