FLEXTODAY, INC. – THIRD-PARTY ADMINISTRATOR PRIVACY POLICY NOTICE - FEBRUARY 2010

CONTACT: Compliance Officer, FlexToday, Inc. 191 W Shaw Ave, Ste 101, Fresno, CA 93704
Ph 559-432-6800 Email Flex@FlexToday.com

FlexToday, Inc. is a third-party administration firm that works under contract with various employers in the administration of their employee benefit plans. Included in the contracts between FlexToday and the Employer is a Business Associate Agreement. This Privacy Policy Notice describes our relationship with your Employer and your health plan, our functions and our policy for the handling of medically-private information.

First, FlexToday works for the Employer that sponsors your benefit plan. FlexToday does not provide benefits nor do we insure, indemnify or fund benefits; we work on behalf of your Employer to provide certain administrative services to assist your Employer in the administration of your health plans. In all cases and in all events related to your benefits or the benefit plan sponsored by your Employer, your Employer will be the "Employer" and the "Plan Administrator" while FlexToday, Inc. is the Business Associate. As a Business Associate working on behalf of your Employer, FlexToday, Inc. is bound by the requirements of HIPAA and the following is our HIPAA Privacy Policy Notice as well as a sample of the HIPAA Business Associate Agreement that is used to direct the procedures followed by your Employer, FlexToday and our handling of medically-private information.

This Notice Describes How Medical Information About You May Be Used and Disclosed and How You Can Get Access To This Information. Please Review This Carefully and Give A Copy To Your Family Or Covered Dependents and Ask Them To Review This Carefully As Well.

We are required by law to protect the privacy of your protected health information, to provide you with this notice of our privacy practices and follow the terms of the notice that is currently in effect. We will not disclose confidential information without your authorization unless it is necessary to provide your health benefits and administer the Plan*{s}*, or as otherwise required or permitted by law. When we need to disclose individually identifiable information, we will follow the policies described in this Notice to protect your confidentiality.

We maintain confidential information and have procedures for accessing and storing confidential records. We restrict internal access to your confidential information to employees who need that information to provide your benefits. We train those individuals on policies and procedures designed to protect your privacy. Our Privacy Officer monitors how we follow those policies and procedures and educates our organization on this important topic.

Who Will Follow This Notice This notice describes the medical information practices of the FlexToday, Inc. in regards to our services on behalf on your Employer, your Employer's group health plan(s) (the "Plan"), and that of any third party that assists in the administration of Plan claims.

Our Pledge Regarding Medical Information We understand that medical information about you and your health is personal. We are committed to protecting medical information about you. We create a record of the health care claims reimbursed under the Plan for Plan administration purposes. This notice applies to all of the medical records we maintain. Your Employer, your personal doctor or other health care provider may have different policies or notices regarding the Employer's use or doctor's use and disclosure of your medical information created in the Employer's office or your doctor's office or clinic.

This notice will tell you about the ways in which we may use and disclose medical information about you. It also describes our obligations and your rights regarding the use and disclosure of medical information.

How We May Use and Disclose Medical Information About You.

The following categories describe different ways that we use and disclose medical information. For each category of uses or disclosures we will explain what we mean and present some examples. Not every use or disclosure in the

category will be listed. However, all of the ways we are permitted to use and disclose information will fall within one of these categories.

For Payment (as described in applicable regulations). We may use and disclose medical information about you to determine eligibility for Plan benefits, to facilitate payment for the treatment and services you receive from health care providers, to determine benefit responsibility under the Plan, or to coordinate Plan coverage. For example, we may share medical information with another entity to assist with the adjudication or subrogation of health claims or to another health plan to coordinate benefit payments.

For Health Care Operations (as described in applicable regulations). We may use and disclose medical information about you for other Plan operations. These uses and disclosures are necessary to run the Plan. For example, we may use medical information in connection with: conducting quality assessment and improvement activities; other activities relating to Plan coverage; conducting or arranging for medical review, legal services, audit services, and fraud and abuse detection programs; business planning and development such as management; and business management and general Plan administrative activities.

To The Employer/Plan Sponsor/Plan Administrator. FlexToday, is the Business Associate working on behalf of the Employer, Plan Sponsor and Plan Administrator to perform various functions of administration, recordkeeping, claims processing and similar ministerial functions and activities. As such, in the performance of those duties, we may disclose health information to the Employer or other third-parties as directed and required by the Employer, subject to the limits of our agreement with the Employer and the Employer's HIPAA policies.

To Business Associates We may contract with individuals or entities known as Business Associates to perform various functions on our behalf or to provide certain services based upon an agreement. In order to perform these functions or to provide these services, Business Associates will receive, create, maintain, use and/or disclose your protected health information, but only after they agree in writing with us to implement appropriate safeguards regarding your protected health information. For example, we may disclose your protected health information to or received your protected health information from a Business Associate to administer claims or provide support services, but only after the Business Associate enters into a Business Associate Agreement with us.

As Required By Law. We will disclose medical information about you when required to do so by federal, state or local law. For example, we may disclose medical information when required by a court order in a litigation proceeding such as a malpractice action. In addition, we are required to disclose your protected health information to the Secretary of the United States Department of Health and Human Services when the Secretary is investigating or determining our compliance with the HIPAA privacy rule.

To Avert a Serious Threat to Health or Safety. We may use and disclose medical information about you when necessary to prevent a serious threat to your health and safety or the health and safety of the public or another person. Any disclosure, however, would only be to someone able to help prevent the threat. For example, we may disclose medical information about you in a proceeding regarding the licensure of a physician.

Disclosures Between Health Plans. In addition to the uses and disclosures of your protected health information for purposes of *treatment, payment* and *health care operations* discussed above, the Plan*{s}* may share your protected health information with each other. The Plan*{s}* have entered into an "organized health care arrangement" to coordinate their operations and to better serve you and the other participants and beneficiaries of the Plan*{s}*. To do this, the Plan*{s}* may need to share protected health information with each other in order to manage their operations. However, the Plan*{s}* will only share your protected health information with each other as is necessary for the *treatment, payment* or *health care operations* of the Plan*{s}* and their common operation.

Disclosure to Health Plan Sponsor. For the purpose of administering the plan, we may disclose to certain employees of the Employer protected health information. Such information may only be used as necessary to comply with the HIPAA requirements, to administer benefits and perform plan administration functions and, if the there is another health plan maintained by the Employer, for purposes of facilitating claims payments under that plan. Your

protected health information cannot be used for employment purposes without your specific authorization.

Military and Veterans. If you are a member of the armed forces, we may release medical information about you as required by military command authorities. We may also release medical information about foreign military personnel to the appropriate foreign military authority.

Workers' Compensation. We may release medical information about you for worker's compensation or similar programs. These programs provide benefits for work-related injuries or illness.

Public Health Risks. We may disclose medical information about you for public health activities. These activities generally include the following:

- to prevent or control disease, injury or disability;
- to report births and deaths;
- to report child abuse or neglect;
- to notify a person who may have been exposed to a disease or may be at risk for contracting or spreading a disease or condition;
- to notify the appropriate government authority if we believe a patient has been the victim of abuse, neglect or domestic violence. We will only make this disclosure if you agree or when required or authorized by law.

Health Oversight Activities. We may disclose medical information to a health oversight agency for activities authorized by the law. These oversight activities include, for example, audits, investigations, inspections, and licensure. These activities are necessary for the government to monitor the health care system, government programs, and compliance with civil rights laws.

Lawsuits and Disputes. If you are involved in a lawsuit or a dispute, we may disclose medical information about you in response to a court or administrative order. We may also disclose medical information about you in response to a subpoena, discovery request, or other lawful process by someone else involved in the dispute, but only if efforts have been made to tell you about the request or to obtain an order protecting the information requested.

Law Enforcement. We may release medical information if asked to do so by a law enforcement official:

- in response to a court order, subpoena, warrant, summons or similar process;
- to identify or locate a suspect, fugitive, material witness, or missing person;
- about the victim of a crime if, under certain limited circumstances, we are unable to obtain the person's agreement;
- about a death we believe may be the result of criminal conduct;
- about criminal conduct at the hospital; and
- in emergency circumstances to report a crime; the location of the crime or victims; or to identify, description or location of the person who committed the crime.

National Security and Intelligence Activities. We may release medical information about you to authorized federal officials for intelligence, counterintelligence, and other national security activities authorized by law.

Inmates. If you are an inmate of a correctional institution or under the custody of a law enforcement official, we may release medical information about you to the correctional institution or law enforcement official. This release would be necessary (1) for the institution to provide you with health care; (2) to protect your health and safety or the health and safety of others; or (3) for the safety and security of the correctional institution.

Disclosures to you. When you request, we are required to disclose to you the portion of your protected health information that contains medical records, billing records, and any other records used to make decision regarding your health care benefits. When requested, we are also required to provide you with an accounting of most disclosures of your protected health information where disclosure was for reasons other than for payment or health care operations, and where the protected health information was not disclosed pursuant to your individual authorization.

Personal Representative. We will disclose your personal health information to individuals authorized by you, or to an individual designated as your personal representative, attorney-in-fact, etc. so long as you provide us with a written authorization or similar supporting documentation. Please note that under the HIPAA privacy rule, we do not have to disclose information to a personal representative if we have a reasonable belief that:

- you have been or may be subjected to domestic violence, abuse or neglect by such person;
- treating such a person as your personal representative could endanger you; or
- in the exercise of professional judgment, it is not in your best interest to treat the person as your personal representative.

Authorizations. We will not use or disclose your confidential information for any purpose other than the purposes described in this Notice, without your written authorization. For example, we will not (1) supply confidential information to another company for its marketing purposes (unless it is for certain limited Health Care Operations), (2) sell your confidential information (unless under strict legal restrictions), or (3) provide your confidential information to a potential employer with whom you are seeking employment without your signed authorization. You may revoke the written authorization at any time, so long as the revocation is in writing, and the revocation shall be effective upon receipt. Any changes in authorization or revocations shall be effective at the time received and will not be effective for any information used or disclosed based upon the previous authorizations.

Your Rights Regarding Medical Information About You

You have the following rights regarding medical information we maintain about you:

Right to Inspect and Copy. You have the right to inspect and copy medical information that may be used to make decisions about your Plan benefits. To inspect and copy medical information that may be used to make decisions about you, you must submit your request in writing to the contact as shown on page 1. If you request a copy of the information, we may charge a fee for the cost of copying, mailing or other supplies associated with your request. We may deny your request to inspect and copy in certain very limited circumstances. If you are denied access to medical information, you may request that the denial be reviewed.

Right to Amend. If you feel that medical information we have about you is incorrect or incomplete, you may ask us to amend the information. You have the right to request an amendment for as long as the information is kept by or for the Plan. To request an amendment, your request must be made in writing and submitted to the CONTACT, shown on page 1. In addition, you must provide a reason that supports your request. We may deny your request for an amendment if it is not in writing or does not include a reason to support the request. In addition, we may deny your request if you ask us to amend information that:

- is not part of the medical information kept by or for the Plan;
- was not created by us, unless the person or entity that created the information is no longer available to make the amendment;
- is not part of the information which you would be permitted to inspect and copy; or
- is accurate and complete.

Right to an Accounting Disclosures. You have the right to request and "accounting of disclosures" where such disclosure was made for any purpose other than treatment, payment, or health care operations. To request this list or accounting of disclosures, you must submit your request in writing to submitted to the CONTACT, shown on page 1. Your request must state a time period which you may not be longer than six years and may not include dates before April, 2003. Your request should indicate in what form you want the list (for example, paper or electronic). The first list you request within a 12-month period will be free. For additional lists, we may charge you for the cost of providing the list. We will notify you of the cost involved and you may choose to withdraw or modify your request at that time before any cost are incurred. You may also request and receive an accounting of disclosures of electronic health records made for payment, treatment, or health care operations during the prior three years for disclosures made on or after (1) January 1, 2014 for electronic health records acquired before January 1. 2009, or (2) January 1, 2011 for electronic

health records acquired on or after January 1, 2009.

Right to Request Restrictions. You have the right to request a restriction or limitation on the medical information we use or disclose about you for treatment, payment or health care operations. You also have the right to request a limit on the medical information we disclose about you to someone who is involved in your care or the payment for your care, like a family member or friend. For example, you could ask that we not use or disclose information about a surgery you had. We are not required to agree to your request. To request restrictions, you must make your request in writing to. In your request, you must tell use (1) what information you want to limit; (2) whether you want to limit our use, disclosure or both; and (3) to whom you want the limits to apply, for example, disclosures to your spouse.

Right to Request Confidential Communications. You have the right to request that we communicate with you about medical matters in a certain way or at a certain location. For example, you can ask that we only contact you at work or by mail. To request confidential communications, you must make your request in writing to FlexToday, shown on page 1. We will not ask you the reason for your request. We will accommodate all reasonable requests. Your request must specify how or where you wish to be contacted.

Right to a 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. Even if you have agreed to receive this notice electronically, you are still entitled to a paper copy of this notice. Please contact the individual identified as the CONTACT on page 1 for the paper copy of this notice.

Changes to This Notice. We reserve the right to change this notice and the effective date of the notice shall be noted on the first page. We reserve the right to make the revised or changed notice effective for medical information we already have about you as well as any information we receive in the future.

Complaints. If you believe your privacy rights have been violated, you may file a complaint with the Employer or with the Secretary of the Department of Health and Human Services. If you wish to file a complaint with the Employer, please submit a written complaint to the contact person listed on page 1 of this notice. All complaints must be submitted in writing. You will not be penalized for filing a complaint. For additional information about HIPAA and your options for filing a complaint with the Office for Civil Rights (OCR), you can call visit their web site, www.hhs.gov/ocr/contact.html, call the OCR toll-free number at (800) 368-1019 or write to them at Office for Civil Rights, U.S. Department of Health and Human Services, 200 Independence Avenue, S.W., Room 509F, HHH Building, Washington, D.C. 20201. For the hearing impaired, please contact the OCR at their toll-free TDD line: (800) 537-7697. As an alternative, you may call the HIPAA toll-free number at (866) 627-7748.

Other uses of Medical Information. Other uses and disclosures of medical information not covered by this notice or the laws that apply to us will be made only with your written permission. If you provide us permission to use or disclose medical information about you, you may revoke that permission, in writing, at any time. If you revoke your permission, we will no longer use or disclose medical information about you for the reasons covered by your written authorization. You understand that we are unable to take back any disclosures we have already made with your permission, and that we are required to retain our records of the care and benefits that we provided to you.

The following is a sample of the Business Associate Agreement between FlexToday, Inc. as the Business Associate and the Employer/Plan Administrator/Plan Sponsor for whom FlexToday, Inc. provides services.

WHEREAS, the Employer offers one or more group health plans (The Plan) as defined in Title 45, Parts 160 and 164 of the Code of Federal Regulations (the "Privacy Regulations") and Title 45, Parts 160, 162 and 164 of the Code of Federal Regulations (the "Security Regulations") (together, the "Privacy and Security Regulations") adopted pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA");
WHEREAS, **FlexToday, Inc., hereafter termed the Business Associate and the Employer** entered into an agreement whereby Business Associate will perform services for the Plan on behalf of the Employer;
WHEREAS, other Employers, Businesses or Entities that that have adopted or will adopt the group health plans (The Plan)

offered by The Employer as a member of a controlled group of corporations, an Affiliated Employer, Predecessor Employer or Successor Employer and, as such, shall also be considered and defined "The Employer" for the purposes of this agreement; and

WHEREAS, the Parties wish to set forth their understandings with regard to the use and disclosure of Protected Health Information ("PHI") by Business Associate in performance of its obligations in compliance with (1) the Privacy and Security Regulations; and (2) Subtitle D of the Health Information Technology for Economic and Clinical Health Act, Title XIII of Public Law 111-005 (42 U.S.C.A. Section 17921 et seq., subchapter III, Privacy) and regulations promulgated thereunder by the U.S. Department of Health and Human Services ("DHHS") (together referred to as "HITECH").

In consideration of the mutual promises set forth below, the parties hereby agree as follows:

1. Definitions. Capitalized terms shall have the meanings given to them in the Privacy and Security Regulations and HITECH, which are incorporated herein by reference.

2. Use and Disclosure of Protected Health Information. The Employer and Business Associate hereby agree to comply with the privacy and security requirements of HIPAA, as set forth in the Privacy and Security Regulations and HITECH. Business Associate shall use and/or disclose PHI only to the extent necessary in furtherance of Business Associate's obligations and duties under the Underlying Agreement with the Plan and as authorized or permitted by the Privacy and Security Regulations and HITECH. Business Associate shall disclose PHI to other business associates of the Plan to the extent necessary for purposes of the Plan's Payment and Health Care Operations, provided such other business associates have business associate agreements in place with the Plan as required by the Privacy Regulations (and a copy of the applicable provisions of such other business associate agreements will be provided to Business Associate upon request). Business Associate shall disclose PHI to the Plan Sponsor to the extent necessary for the Plan Sponsor's administration activities that constitute Payment or Health Care Operations, provided the Plan document has been amended as required by the Privacy Regulations (and a copy of the applicable provisions of the Plan document will be provided to Business Associate upon request). Business Associate may disclose Summary Health Information to the Plan Sponsor for the purpose of (a) obtaining bids for health or stop loss insurance for the Plan, or (b) modifying, amending or terminating the Plan.

3. **Prohibition on Unauthorized Use or Disclosure of PHI. Business Associate shall not use or disclose any PHI received from or on behalf of the Plan, except as permitted or required by the Underlying Agreement, this Agreement, the Privacy and Security Regulations, HITECH and as required by law or as otherwise authorized in writing by the Plan. Business Associate shall comply with the applicable provisions of:**

(a) the Privacy Regulations;

(b) HITECH (including 42 U.S.C.A. sections 17931 and 17934);

(c) state laws, rules and regulations applicable to individually-identifiable health information not preempted by federal law; and (d) the Plan's health information privacy policies and procedures.

4. **Business Associate's Operations. Business Associate may use PHI it creates for or receives from the Plan, in its capacity as a Business Associate, to the extent necessary for Business Associate's proper management and administration or to carry out Business Associate's legal responsibilities but only if:**

(a) The disclosure is required by law; or

(b) Business Associate obtains reasonable assurance, evidenced by written contract, from any person or organization to which Business Associate shall disclose such PHI that such person or organization shall:

(i) Hold such PHI in confidence and use or further disclose it only for the purpose for which Business Associate disclosed it to the person or organization or as required by law; and

(ii) Notify Business Associate (who shall in turn promptly notify the Plan) of any instance of which the person or organization becomes aware in which the confidentiality of such PHI was breached as soon as possible.

5. Data Aggregation Services. Business Associate may use PHI to provide Data Aggregation Services related to the Plan's Health Care Operations.

6. PHI Safeguards. Business Associate shall develop, implement, maintain and use appropriate administrative, technical

FlexToday, Inc.
HIPAA Privacy Policy Notice

and physical safeguards to prevent the improper use or disclosure of any PHI relating to the Plan.

7. Electronic Health Information Security and Integrity. Business Associate shall develop, implement, maintain and use appropriate administrative, technical and physical security measures consistent with and in compliance with the Security Regulations and HITECH to preserve the integrity, confidentiality and availability of all electronic PHI that it creates, receives, maintains or transmits on behalf of the Plan. Business Associate shall document and keep these security measures current in accordance with the Security Regulations and HITECH (including 42 U.S.C.A. section 17931).

8. Protection of Exchanged Information in Electronic Transactions. If Business Associate conducts any Standard Transaction for or on behalf of the Plan, Business Associate shall comply, and shall require any subcontractor or agent conducting such Standard Transaction to comply, with each applicable requirement of the Privacy and Security Regulations.

9. Subcontractors and Agents. Business Associate shall require each of its subcontractors or agents to whom Business Associate may provide PHI on behalf of the Plan to agree to written contractual provisions that impose at least the same obligations to protect such PHI as are imposed on Business Associate by this Agreement, the Privacy and Security Regulations and HITECH.

10. Access to PHI. Business Associate shall provide access, at the request of the Plan, to PHI in a Designated Record Set, to the Plan or, as directed by the Plan, to an Individual to meet the requirements under Title 45, Section 164.524 of the CFR or applicable state law and to meet the electronic transmission requirements for access to Electronic Health Records by Individuals in accordance with HITECH, including 42 U.S.C.A. section 17935(e). Business Associate shall provide access in the time and manner set forth in the Plan's health information privacy policies and procedures.

11. Amending PHI. Business Associate shall make any amendment(s) to PHI in a Designated Record Set that the Plan directs or agrees to pursuant to Title 45, Section 164.526 of the CFR at the request of the Plan or an Individual in the time and manner set forth in the Plan's health information privacy policies and procedures.

12. Accounting for Disclosures of PHI.

(a) Business Associate shall document all disclosures of PHI and information related to such disclosures as would be required for the Plan to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with Title 45, Section 164.528 of the CFR, including PHI in Electronic Health Records in accordance with HITECH.

(b) Business Associate agrees to provide the Plan, in the time and manner set forth in the Plan's health information privacy policies and procedures, information collected in accordance with Section 12(a) above, to permit the Plan to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with Title 45, Section 164.528 of the CFR and HITECH, including 42 U.S.C.A. section 17935(c) with respect to Electronic Health Records. To the extent a request for an accounting relates to disclosures of PHI in Electronic Health Records by Business Associate, at the Plan's election, the Plan can provide an Individual who requests such accounting with Business Associate's contact information, and Business Associate shall provide the accounting directly to the Individual upon request by the Individual.

13. Access to Books and Records. Business Associate shall make its internal practices, books and records relating to the use and disclosure of PHI received from or on behalf of the Plan available to the Plan and to DHHS or its designee for the purpose of determining the Plan's compliance with the Privacy Regulations and HITECH.

14. Reporting. As described below, Business Associate shall report to the Plan in writing (a) any use or disclosure of PHI not permitted under 45 CFR section 164, Subpart E, this Agreement, or by law, (b) any Security Incident of which it becomes aware and (c) any Breach of Unsecured PHI in accordance with HITECH, including 42 U.S.C.A. section 17932. For purposes of this Agreement, the term Security Incident means the attempted or successful unauthorized access, use, disclosure, modification or destruction of electronic PHI relating to the Plan.

(a) Reporting Security Incidents or Improper Uses or Disclosures. Business Associate shall make the report to the Plan's Privacy Official (or to the Plan's Security Official in the event of a Security Incident) within 3 business days after Business Associate learns of such unauthorized use or disclosure or Security Incident. Business Associate's report shall:

(i) identify the nature of the unauthorized use or disclosure or Security Incident;

(ii) identify the PHI affected;

(iii) identify who made the unauthorized use and/or received the unauthorized disclosure and/or participated in the Security Incident, if known;

(iv) identify what Business Associate has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure or Security Incident; (v) identify what corrective action Business Associate has taken or shall take to prevent future similar unauthorized use or disclosure or Security Incident; and

(vi) provide such other information, including a written report, as reasonably requested by the Plan's Privacy Official or Security Official. Any Security Incident or unauthorized use or disclosure of PHI that is a Breach of Unsecured PHI shall be reported as required under subsection (b) below.

(b) Notification of a Breach. Pursuant to HITECH, including 42 U.S.C.A. section 17932, and regulations under 45 CFR Parts 160 and 164, as amended, Business Associate shall provide written notice to the Plan's Privacy Official of any Breach of Unsecured PHI within three business days after Business Associate discovers the Breach. Business Associate shall conduct the risk assessment to determine whether a Breach occurred. Business Associate's report to the Plan shall identify or describe:

(i) the affected Individual whose Unsecured PHI has been or is reasonably believed to have been accessed, acquired or disclosed;

(ii) the incident, including the date of the Breach and the date of the discovery of the Breach, if known;

(iii) who made the unauthorized use and/or received the unauthorized disclosure;

(iv) the types of Unsecured PHI involved in the Breach;

(v) any specific steps the Individual should take to protect him or herself from potential harm related to the Breach;

(vi) what the Business Associate is doing to investigate the Breach, to mitigate losses and to protect against further Breaches;

(vii) contact procedures for how the Individual can obtain further information from the Business Associate; and

(viii) such other information, including the risk assessment analysis prepared by the Business Associate, as reasonably requested by the Plan's Privacy Official.

15. Sale of PHI. Business Associate shall not receive direct or indirect payment in exchange for any PHI relating to the Plan or its Individuals, including Electronic Health Records, unless Business Associate receives authorization by all affected Individuals, except as permitted under HITECH including 42 U.S.C.A. section 17935(d).

16. Marketing. Business Associate shall not receive direct or indirect payment for marketing communications which include PHI relating to the Plan or its Individuals without authorization from the affected Individuals unless such communication is permitted under the Privacy Regulations and HITECH, including 42 U.S.C.A. section 17936.

17. Restrictions on Uses, Disclosures and Requests.

(a) Business Associate will limit all uses, disclosures and requests of PHI, including electronic PHI, to the Limited Data Set to the extent possible or, if that is not sufficient, then to the minimum necessary to accomplish the intended purpose of such use, disclosure or request, as required by the Privacy Regulations and HITECH (including 42 U.S.C.A. 17935(b)).

(b) Upon the request of an Individual, Business Associate will not disclose such Individual's PHI for purposes of Payment or Health Care Operations if the Individual paid in full out of pocket for the health care item or service to which the PHI relates, in accordance with HITECH (including 42 U.S.C.A. section 17935(a)).

18. Mitigation. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of the requirements of this Agreement.

19. Termination for Cause. As required by the Privacy Regulations and section 42 U.S.C.A. 17934, if the Plan or Business Associate ("Non-Breaching Party") becomes aware that the other entity to this Agreement has engaged in a material breach ("Breaching Party"), then the Non-Breaching Party shall:

(a) Provide an opportunity for the Breaching Party to cure the breach or end the violation and terminate this Agreement and the Underlying Agreement if the Breaching Party does not cure the breach or end the violation within the time specified by the Non-Breaching Party.

(b) Immediately terminate this Agreement and the Underlying Agreement if cure is not possible.

(c) If neither termination of this Agreement and the Underlying Agreement nor cure is feasible, report the violation to

DHHS.

20. Return or Destruction of Health Information.

(a) Except as provided in Section 20(b) below, and subject to any record retention provisions of the Underlying Agreement, upon termination, cancellation, expiration or other conclusion of this Agreement and the Underlying Agreement, Business Associate shall return to the Plan or destroy all PHI created or received by Business Associate on behalf of the Plan. This provision shall also apply to PHI that is in the possession of subcontractors or agents of Business Associate.

(b) In the event that the Parties mutually determine that returning or destroying the PHI is infeasible, Business Associate shall retain the PHI, extend the protections of this Agreement to such PHI and maintain the confidentiality of all such PHI, for so long as Business Associate maintains such PHI. The obligations of Business Associate under this Section 20(b) shall survive termination of this Agreement and the Underlying Agreement.

Notice is hereby provided that the Business Associate has determined that returning or destroying benefit claims and related information received from participants (including the spouse, dependent(s) and health care providers of the participant) in the Internal Revenue Code Section 125 "Flex Plan" (to include but not limited to the Medical Flex Spending Account and Dependent Care Assistance Plan), Health Reimbursement Arrangement (HRA) or other Welfare Benefit Plan of the Covered Entity is infeasible. Efforts will be made to destroy the information that is readily accessible. However, much of this information, in both electronic and in physical forms, is intermingled with the electronic and physical information of other entities, unrelated to the Covered Entity, with whom the Business Associate has similar working relationship.

21. Obligations of Plan.

(a) The Plan shall provide Business Associate a copy of the Plan's Notice of Privacy Practices.

(b) The Plan shall notify Business Associate of any restriction to the use or disclosure of PHI that the Plan has agreed to (and any revocation of such a restriction), to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

(c) The Plan shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy Regulations or HITECH if done by the Plan, except as permitted in Sections 4 and 5 above.

22. Automatic Amendment. Upon the effective date of any amendment to the Privacy and Security Regulations or HITECH and any applicable regulations thereunder with respect to PHI, the Agreement shall automatically be deemed to be amended to incorporate such amendment to the Privacy and Security Regulations and HITECH and applicable regulations so that Business Associate and the Plan remain in compliance with the Privacy and Security Regulations and HITECH and applicable regulations.

21. Hold Harmless. Business Associate shall indemnify and hold the Plan and its employees, directors and trustees harmless from all liabilities, penalties, taxes, costs, expenses or damages of any sort resulting from or attributable to Business Associate's breach of this Agreement.

22. Counterparts. This Agreement may be executed in any number of counterparts, each of which shall be deemed an original and such counterparts shall constitute one and the same instrument.

FlexToday, Inc.
HIPAA Privacy Policy Notice