

**LEVY COUNTY, a Political  
Subdivision of the State of  
Florida**

**PUBLIC RISK  
MANAGEMENT OF  
FLORIDA**

Privacy Policy and Procedures

## Table of Contents

INTRODUCTION .....	3
PERSONNEL DESIGNATIONS .....	5
RESTRICTED INTERNAL ACCESS TO PROTECTED HEALTH INFORMATION .....	7
USES AND DISCLOSURES THAT ARE REQUIRED BY STATUTE OR PERMITTED BY AUTHORIZATION .....	12
USES AND DISCLOSURES PERMITTED FOR REASONS OTHER THAN TREATMENT, PAYMENT AND HEALTH CARE OPERATIONS WITHOUT INDIVIDUAL AUTHORIZATION. ....	17
THE MINIMUM NECESSARY REQUIREMENT .....	21
DE-IDENTIFICATION POLICY .....	23
BUSINESS ASSOCIATE RELATIONSHIPS .....	25
BREACHES OF UNSECURED PROTECTED HEALTH INFORMATION .....	27
REQUESTS TO RESTRICT USES AND DISCLOSURES .....	29
REQUESTS BY INDIVIDUALS TO INSPECT AND COPY THE DESIGNATED RECORD SET (DRS) .....	31
REQUESTS FOR CONFIDENTIAL COMMUNICATIONS OF PHI AND/OR ALTERNATIVE MEANS .....	36
ACCOUNTING OF DISCLOSURES OF PHI .....	38
AMENDMENT REQUESTS .....	42
POLICY SUBJECT: COMPLAINTS .....	47
MITIGATION .....	49
NON-RETALIATION .....	50
TRAINING .....	51
NOTICE OF PRIVACY PRACTICES; DISSEMINATION; CHANGES .....	52
ENFORCEMENT; SANCTIONS FOR NON-COMPLIANCE .....	55
DOCUMENTATION AND RECORDS RETENTION .....	57

ADDENDUM A	Authorized Employees
ADDENDUM B	Family Authorization to Use or Disclose PHI Form
ADDENDUM C	General Authorization to Use or Disclose PHI Form
ADDENDUM D	Authorization to Healthcare Provider to disclose PHI to the Company
ADDENDUM E	Notice of Privacy Practices

## INTRODUCTION

**Levy County, a political subdivision of the State of Florida** is the Plan Sponsor (“Plan Sponsor”) and acting as the Plan Administrator, is responsible for administering health care benefits. For purposes of the Privacy Rule, the **Public Risk Management of Florida** (the “Plan”) covers health care benefits consisting of Medical Benefits (including Post-Retirement Benefits) and Prescription Drug Benefits (“collectively referred to as “Medical Benefits”). If the Plan Sponsor offers other health care benefits, including Dental, Vision, Employee Assistance Program and/or Health Care Flexible Spending Account, then these Policies and Procedures also apply.

In performing its Medical Benefits functions, the Plan Administrator has delegated the day-to-day administration of most Plan benefits to a third party administrator, Florida Blue (TPA) and to a lesser extent to employees of the Plan Sponsor and other third parties, including Public Risk Management of Florida Group Health Trust. Florida Blue has been named Claims Fiduciary for the Medical Benefits and, therefore has full and final responsibility for claim determination and administration for the Medical Benefits. If a third party provides services that are related to the Medical Benefits, the third party is referred to as a “Business Associate.”

The Plan Sponsor, the Plan Sponsor Employees and the Business Associates request, receive, use, store and disclose individually identifiable medical information about participants and their dependents for the purpose of administering the Medical Benefits. Therefore, the individually identifiable medical information received and stored by the Plan Sponsor, the Plan Sponsor Employees and the Business Associates in the administration of the Medical Benefits is protected health information (“PHI”) and is protected by HIPAA. The Plan will designate certain Plan Sponsor Employees who are authorized to handle and protect PHI on behalf of the Plan; said employees will be referred to as “Authorized Employees”.

The Plan Sponsor, as an employer, requests, receives and stores medical information about its employees for a variety of purposes, including pre-employment and employment testing (including, in some instances, drug screening) and determining whether an employee is eligible for worker’s compensation benefits, leave benefits including, but not limited to those under the Family and Medical Leave Act or an accommodation under the Americans’ with Disabilities Act. The Plan Sponsor receives this information either voluntarily from the employee or directly from the employee’s health care provider. Therefore, the medical information received and stored by the Plan Sponsor in its role as the employer is not PHI and is not protected by HIPAA after its disclosure.

## I. PRIVACY POLICY STATEMENT

These policies and procedures are designed and intended to ensure the Plan's<sup>1</sup> compliance with the Health Insurance Portability and Accountability Act ("HIPAA") Standards for Privacy of Individually Identifiable Health Information (the "Privacy Rule"). The Plan adopts these policies and procedures to protect the individually identifiable health information that it creates and maintains from unauthorized use, disclosure, or access, and to maintain the confidentiality and integrity of that protected health information ("PHI"). These policies and procedures also ensure that individuals have rights related to their PHI.

Through the Notice of Privacy Practices ("Privacy Notice") that the Plan disseminates to its participants, individuals are informed of the Plan's legal duties and privacy policies and procedures. The Privacy Notice also informs them of their individual rights with respect to their PHI. The Privacy Notice will be updated as necessary from time to time and revisions disseminated to Plan Participants.

These policies and procedures will be amended and/or supplemented as necessary and appropriate to comply with changes in the law or regulations or other interpretation of the Plan's privacy-related obligations, or to reflect changes related to the Plan or the internal structure of the Plan Sponsor. The Plan will promptly document and implement these policies and procedures, including revising the Privacy Notice whenever there is a change in the law, regulations or interpretation of the Plan's privacy obligations and/or a material change to the uses or disclosures of PHI or other privacy practices that necessitate a change in these policies and procedures. If a change (other than a change in provisions) requires the revision and dissemination of a new Privacy Notice, the Plan will not implement this change before the effective date of the revised Privacy Notice unless the Privacy Officer deems it necessary to apply the change to PHI that the Plan created or received before this effective date.

References in these policies and procedures to the "Plan Administrator" refer to the Plan Sponsor in its capacity as the plan administrator of the Medical Benefits.

---

<sup>1</sup> The term "ensure" as used throughout these Policy and Procedures is not meant to guarantee compliance with the Privacy Rule. Rather, "ensure" shall mean the Privacy Officer, Plan Sponsor Employees, Business Associates or others, as applicable, will use their best efforts to comply with the Privacy Rule.

II. **POLICY SUBJECT: PERSONNEL DESIGNATIONS**

**POLICY:** The Plan Administrator has designated a Privacy Officer to assume the responsibilities and perform the duties as described below.

A. **PRIVACY OFFICER DESIGNATION**

The Plan Administrator has designated a Privacy Officer who is responsible for overseeing and directing the development and implementation of the Plan's privacy policies and procedures in compliance with HIPAA's Privacy Rule.

1. **Designated Privacy Officer.**

**Jacqueline Martin, Human Resource Manager**  
**Levy County Board of County Commissioners**  
**PO Box 310**  
**Bronson, FL 32621**  
martin-jacqueline@levycounty.org

- a. **Qualifications.** The Privacy Officer is a Plan Sponsor Employee who possesses a sufficient amount of authority within the Plan Sponsor to cause the Plan Sponsor, if necessary, to be accountable for implementing, following and changing its policies and practices to comply with the requirements of HIPAA.
2. **Duties and Responsibilities of the Privacy Officer.** The Privacy Officer is responsible either directly or by his/her delegated authority, for monitoring and ensuring the Plan's compliance with the HIPAA Privacy Rule and these policies and procedures. Specifically, the Privacy Officer will:
- a. Oversee the development and implementation of HIPAA compliance policies and procedures which include document maintenance and retention, administrative, physical and technical safeguards for handling PHI, the handling of individual requests for access, amendments and disclosure of PHI; review and revise the policies and procedures as required or needed for continued compliance with the HIPAA Privacy Rule; communicate these policies and procedures and any revisions or updates to all Authorized Employees.
- b. Develop and distribute appropriate forms to use, such as for example, for individual requests for access to PHI, confidentiality agreements for Authorized Employees and monitor the use and storage of said forms.
- c. Coordinate with departments throughout the Plan Sponsor to identify all HIPAA non-compliant processes and systems, and to develop and implement those changes necessary to ensure all processes and systems are HIPAA compliant.

- d. Serve as central liaison for internal departments of Plan Sponsor involved in HIPAA systems and processes, and for external business partners and vendors involved in HIPAA systems and processes.
- e. Prepare Plan Sponsor budgets for HIPAA compliance.
- f. Respond to inquiries and requests from individuals, government officials, and other third parties regarding uses and disclosures of PHI, or more generally about these policies and procedures and promptly renders determinations in response to such inquiries and requests.
- g. Oversee workforce training on HIPAA compliance; ensure that all Authorized Employees are trained in accordance with these Policies and Procedures and maintain record keeping of all training.
- h. Ensure that the Plan's Notice of Privacy Practices ("Privacy Notice") is timely disseminated to individual participants, and review and revise the Privacy Notice to reflect any changes to the law or the Plan's privacy policies and procedures or practices.
- i. Establish a complaint procedure, investigate or oversee the investigation of any complaints that allege that the Plan, the Plan Administrator, a Plan Sponsor Employee or a Business Associate has not complied with or has violated these policies and procedures
- j. Retain copies of all complaints and their resolution, and copies of all disclosures of PHI in accordance with the policies on Controls on Access and on Documentation set forth below which must be followed at all times.
- k. Develop procedures for the identification, investigation and notification of potential breaches of unsecured PHI.
- l. In his/her absence, the HIPAA Privacy Officer may delegate some of the duties described above to an Authorized Employee.

**B. DOCUMENTATION.** Documentation related to these personnel designations will be retained for 6 years in accordance with 45 C.F.R. §164.530(j), and Policy XX.

### **III. POLICY SUBJECT: RESTRICTED INTERNAL ACCESS TO PROTECTED HEALTH INFORMATION**

**POLICY:** The Plan Administrator has implemented reasonable safeguards, including appropriate administrative, technical and physical measures, to protect the privacy of PHI, and to prevent impermissible uses and disclosures of PHI. The Plan Administrator and the Plan Sponsor have granted limited access of PHI to only those Plan Sponsor Employees who need PHI to carry out their duties. These Plan Sponsor Employees are referred to as “Authorized Employees”.

#### **A. CONTROLS ON ACCESS**

The Plan Sponsor shall maintain the following standard practices of administrative, technical and physical safeguards for the housing and securing of PHI:

##### **Physical protection of files containing PHI:**

All file cabinets housing personnel records must be kept locked at all times.

All files containing PHI must be separated from personnel record and files related to non-health benefits (e.g. disability or life insurance), kept in designated HIPAA filing cabinets with keys safeguarded by the Privacy Officer, or a designated Authorized Employee. If other Authorized Employees need access to the PHI in the designated HIPAA cabinet, the safeguarding Authorized Employee has to provide the key and retrieve it once the other Authorized Employees have completed their use of the PHI in said cabinet.

Any offices or records rooms containing HIPAA cabinets designated for PHI should be locked at the end of each workday.

PHI may not be left out in non-secure areas. When they leave their desk, Authorized Employees must close up any PHI at their desks and place it in a locked desk drawer or in the designated locked cabinet.

Any document containing PHI provided by an employee, on or after April 14, 2003, that does not require intervention by an Authorized Employee should be returned to the employee, maintained in a confidential HIPAA file, or archived.

Any documentation containing PHI provided by an employee, on or after April 14, 2003, that does require intervention by an Authorized Employee should contain documentation of the activity required and maintained in the HIPAA file for at least 6 years.

Any document containing PHI provided by an employee dated prior to April 14, 2003 may be shredded or archived.

Any forms older than 1996 may be shredded or archived. All outdated reports and spreadsheets that include PHI, such as enrollment data, should be deleted from databases and, if necessary, placed on a disk and kept in a locked desk or file cabinet.

**Secure Equipment and Systems:**

A separate, dedicated fax machine for transmitting or receiving any data that constitutes PHI should be maintained. In the alternative, procedures must be established so that an Authorized Employee is notified in advance of the transmittal of PHI and is there to collect it upon its transmittal.

Copying of PHI should be performed directly by the relevant Authorized Employee and copies should be limited to the minimum necessary to accomplish the task at hand. When copying is done, all PHI must be removed off the machine.

If Authorized Employees use the e-mail system to communicate PHI the system must be protected by passwords or field restrictions and firewalls.

For example, correspondence regarding claims payments or enrollment information with a carrier or TPA.

All computers that house or could house PHI must have adequately functioning screen shutdowns. Authorized Employees may only have PHI open on their computers if they are working with PHI and must not leave PHI open on their system if they leave their desk for any amount of time.

IT employees may have incidental access to PHI on the company e-mail system because they monitor the system and store the e-mail back-up tapes. Authorized Employees should ensure that the IT employees are aware not to use or disclose any PHI that they incidentally have access to via the company e-mail system. If access is more than incidental, Authorized Employees should contact the Privacy Officer.

**Mail:**

All mail personally addressed to Human Resource Manager, mailed from a Carrier or TPA, should be opened by the Privacy Officer, or Authorized Employee addressee. Mail may be sorted but not opened by non- Authorized Employees.

**Secure Conversations:**

Authorized Employees may only discuss PHI with each other to the extent necessary to perform their duties.

Authorized Employees may not discuss PHI with or transmit PHI to non-Authorized Employees except if permitted by the Policies and Procedures or if written authorization is obtained by the individual allowing discussion with a non-Authorized Employee.

Any teleconferences or meetings with other Authorized Employees where PHI is or may be discussed must be held in private and closed rooms, with only Authorized Employees present and the individual whose PHI is being discussed.

If an individual telephones an Authorized Employee for assistance, the Authorized Employee must verify that individual's identity by requesting the date of birth of the participant. If the assistance requested requires that the Individual has signed an appropriate authorization form, the Authorized Employee will verify that the proper authorization is in place. If not, the Authorized Employee will not provide the requested assistance until the required authorization form is signed and delivered to the Authorized Employee.

**Overlapping duties:**

To the extent that the Authorized Employees' job responsibilities overlap between (i) the Medical Benefits of the Plan and any non-Medical Benefits or retirement plans or (ii) between the Medical Benefits of the Plan and other employer functions, Authorized Employees must not use PHI to make decisions related to non-Medical Benefits, retirement plans or other employer functions unless authorized by the individual or otherwise permitted by the Policies and Procedures or the Privacy Rule and approved by the Privacy Officer.

- For instance, PHI derived from the Plan must not be used in making decisions relating to FMLA or disability leave, or to initiate a disability pension.

**B. PERSONS AUTHORIZED TO ACCESS PHI; PURPOSES AND CONTROLS ON ACCESS.**

Refer to Addendum A for a list of the Authorized Employees who are authorized to have access to the following categories/types of PHI for only the purpose(s) listed and after the listed controls on access are met. Note: The Privacy Officer is considered an Authorized Employee.

**PHI: Claim information, enrollment information, utilization information from vendors, payment information; PHI provided by individuals seeking assistance with a claim and any other PHI provided by health provider or Business Associate related to the individual's inquiry.**

**Purpose: Maintain the daily administrative functions of the healthcare plans and ensure the quality of service and overall integrity of the Plan including:**

- ❗ Reconciling and funding claim accounts.
- ❗ Calculating and applying appropriate charges.
- ❗ Verifying correct billing.
- ❗ Substantiating costs as required by cost accounting standards applicable to Government Contracts. Assistance in claim and payment resolution as a last resort if resolution unsuccessful after contacting Business Associates.
- ❗ Provide coverage verification for HCFA requests, court orders, and Medicare secondary payor program information.
- ❗ Assist an individual with a claim after contacts with the health provider or TPA have failed to achieve resolution.
- ❗ Any purpose for PHI described below as applicable to the Participating Employers.
- ❗ Any other uses and disclosures as permitted under this Policy and Procedures document.

**Access Controls:** Use the minimum necessary guidelines when accessing and sharing PHI and follow guidelines as outlined in Policy III.A of this document.

**PHI: Written documentation containing PHI provided by employees, and subsequent communication with a carrier to TPA on issues related to protected health benefits under the Plan.**

**Purpose:** Assistance with claim resolution, explanation of benefits, clarification of payment/coverage.

**Access Controls:** All inquiries should only be initiated by the individual. Only the minimum necessary amount of information should be shared. Inquiries should first be directed to the carrier and/or TPA. Any correspondence should be documented and maintained in the HIPAA file cabinet. All electronic correspondence should be printed, documented and kept in HIPAA files, and deleted from e-files.

**PHI: Benefit Election and Coverage Information**

**Purpose:** Confirm benefit coverage for various court orders, medical support documentation, HCFA inquiries, Medicare secondary payor program and clarification of payment/coverage for provider offices (doctors, dentists) who inquire.

For example, if individual or covered dependent is in a provider office and does not have his/her ID card.

**Access Controls:** All inquiries must be forwarded to the TPA, as HR does not readily house this information. The minimum necessary guidelines should be adhered to along with procedures outlined in Policy III.A of this document.

**PHI: Enrollment data requests made to TPA by Authorized Employee in Human Resources**

**Purpose:** To assist in special projects such as preparation of:

- Termination documents
- Lay-off documents
- Merger and Acquisition due diligence documentation
- Divestiture documentation
- Special 'one-off' projects.

**Access Controls:** All inquiries must be initiated by the appropriate Authorized Employee. The minimum necessary guidelines should be adhered to along with procedures outlined in Policy III.A of this document.

Electronic information should be shared in the form of confidential, password-protected reports.

**PHI: Monthly billing reports prepared by TPA**

**Purpose:** Process monthly fringe charge-back for benefit utilization and to verify the accuracy of the billing.

**Access Controls:** Information should be shared in the form of confidential, password protected reports or system access. Any faxes should be faxed directly to the authorized plan sponsor employee to a private fax machine. Hardcopy reports should be maintained in a confidential, locked file cabinet or office. Photocopies of the report should be kept at a minimum. The minimum necessary guidelines should be adhered to along with procedures outlined in Policy III.A of this document.

**PHI: 2002 (or older) medical and flex enrollment forms.**

**Purpose:** Reference purposes, HCFA and SSA form completion.

**Access Controls:** All forms must be kept in files separate from the personnel file, in locked cabinets and locked offices.

**IMPORTANT: UNLESS SPECIFICALLY AUTHORIZED AS ABOVE OR IN WRITING BY THE PRIVACY OFFICER OR ASSOCIATE PRIVACY OFFICER, ALL OTHER ACCESS TO PROTECTED HEALTH INFORMATION IS UNAUTHORIZED, STRICTLY PROHIBITED AND MAY RESULT IN SANCTIONS.**

**IV. POLICY SUBJECT: USES AND DISCLOSURES THAT ARE REQUIRED BY STATUTE OR PERMITTED BY AUTHORIZATION**

**POLICY:** The Plan, the Authorized Employees and the Business Associates, will use or disclose PHI only as permitted by the Privacy Rule. The Plan will permit an individual's PHI to be used or disclosed for purposes of treatment, payment or health care operations as defined in 45 C.F.R. §164.501. In addition, the Privacy Officer will allow authorized persons to have access to PHI, in accordance with this Policy, to use or disclose PHI only to the extent provided in this section, and in accordance with the minimum necessary requirements set out in 45 C.F.R. §164.514(d) and Policy VI.

A. **REQUIRED USES AND DISCLOSURES.** The Plan will use or disclose PHI in the following circumstances, as is required by 45 C.F.R. §164.502(a)(2):

1. **Individual Access-** must be given to the individual who is the subject of the PHI contained in the designated record set, as defined in 45 C.F.R. §164.501, (i.e. enrollment, payment, claims adjudication records as well as any PHI used to make coverage decisions).

2. **Family Access**

a. Parents and/or guardians of minor children:

In the normal course, parents and/or guardians ("parents") are considered the personal representatives of unemancipated minors. As such, the Plan generally responds to parental inquiries about their children's treatment, and provides parents with access to the minor's PHI. However, the Plan does not respond to inquiries from parents of children who are 18 years of age or older without an authorization as described below from the child. In addition, the Plan does not respond to parental inquiries about reproductive health services, HIV/AIDS treatment, or mental health treatment that has been provided to a child until the Plan has had the opportunity to review any applicable state law to ensure that the Plan may respond to the parental inquiry.

b. Family/adult children and other persons:

In order to facilitate the disclosure of PHI of a participant, a spouse or an adult dependent to any one other of the above, individuals will be asked to complete the form "Family Authorization to Disclose Protected Health Information" as attached in Addendum B to these Policies and Procedures. Alternatively, an individual may complete an authorization each time they wish specific PHI disclosed to a family member or other person., using the general authorization form attached as Addendum C.

3. **Access by Secretary of HHS.** To the Secretary of the Department of Health and Human Services (“HHS”) when the Secretary is investigating a complaint or monitoring compliance. The Plan will verify the identity of the HHS requester as set forth in Policy V.B.2.

**B. USES AND DISCLOSURES PERMITTED FOR TREATMENT, PAYMENT OR HEALTH CARE OPERATIONS.** The Plan uses or discloses PHI for purposes of treatment, payment or health care operations. **No written authorization or consent is required for these uses or disclosures.**

1. **Treatment.** The Plan may use or disclose PHI for treatment purposes to assist any healthcare provider in that provider’s treatment activities; or to coordinate or manage with a health care provider to provide treatment for an individual. However, the Plan does not foresee any circumstances for making such disclosures.
2. **Payment.** For payment purposes, the Plan may use or disclose PHI to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or to obtain or provide reimbursement for the provision of health care. These payment activities must relate to an individual, and include, but are not limited to:
  - a. Determination of eligibility or coverage, including the coordination of benefits and determination of cost sharing amounts, adjudication or subrogation of health benefit claims;
  - b. Risk adjustment based on enrollee health status and demographic characteristics;
  - c. Billing, claims management, collection activities, obtaining payment under a contract for reinsurance, including stop-loss insurance and excess of loss insurance, and related health care data processing;
  - d. Review of health care services with respect to medical necessity, coverage under the Plan, appropriateness of care, or justification of charges;
  - e. Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and
  - f. Disclosure to consumer reporting agencies of any of the following PHI relating to the collection of premiums or reimbursement: name and address; date of birth; social security number; payment history; account number; and name and address of the Plan.
3. **Health Care Operations.** The Plan may use or disclose PHI for the following activities:
  - a. Except as prohibited by 45 C.F.R. §164.502(a)(5)(i) and Policy IV.D, underwriting, enrollment, premium rating, and other activities related to renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health insurance, including stop-loss insurance and excess of loss

insurance. However, if such health insurance or health benefits are not placed with the health insurance carrier, then the health insurance carrier will not use or disclose that PHI for any other purpose;

- b. Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
- c. Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and
- d. Business management and general administrative activities of the Plan, including, but not limited to:
  - (i) Management activities related to implementing and complying with the Privacy Rule;
  - (ii) Customer service, including the provision of data analyses for policy holders or other customers, provided that PHI is not disclosed to the policy holder or other customers;
  - (iii) Resolution of internal grievances; and
  - (iv) Due diligence in connection with the sale or transfer of assets to a potential successor.

**C. USE AND DISCLOSURE OF PHI TO A THIRD PARTY PERMITTED PURSUANT TO A VALID AUTHORIZATION.**

- 1. **Requirement.** The Plan will use or disclose PHI only upon receipt of a valid authorization as provided for in Addendum C of this document for purposes other than payment, treatment or health care operations, or reasons other than those specified in the Privacy Rule as not requiring consent or authorization or otherwise required by law. Once a valid authorization is received, the Plan will only use and disclose information in a manner consistent with the terms of the authorization.

**Authorization Forms.** Upon written or oral request, the Authorized Employee handling the request will provide individuals with the required Authorization Form set forth in either Addendum B or C to these Policies and Procedures, as may be applicable.

**2. Procedure To Obtain or Revoke Authorizations**

- a. For certain PHI to be used or disclosed at an individual's request, the following procedure is to be followed:
  - (i) The individual must contact the HIPAA Contact Person at his/her location or other Authorized Employee orally or in writing to request an Authorization Form.

- (ii) In response, the Authorized Employee will provide or forward an Authorization Form to be filled out and signed by the individual.
  - (iii) If the individual submits a deficient or incomplete authorization form, the Authorized Employee will contact that individual, orally or in writing, to explain why the Authorization is deficient and instruct the individual on how to correctly complete the Authorization Form.
- b. If the Plan seeks to have an individual sign an Authorization, the following procedure will be followed:
  - (i) The Plan will send the individual a written request stating the proposed reason for the use or disclosure of the information, and enclose an appropriate Authorization Form to be completed and signed by the individual.
  - (ii) The Plan will provide the individual with a copy of his/her executed authorization when an original is received.
  - (iii) Thereafter, the HIPAA Contact Person will ensure that the correct PHI is used or disclosed in accordance with the Authorization.
- c. **Authorization Revocation.** An individual may revoke, in writing, his/her signed authorization at any time, except as follows (45 C.F.R. §164.508(b)(5)):
  - (i) To the extent that the Plan has taken action in reliance on the authorization prior to revocation. If there is a question as to whether the Plan has relied on the authorization so that revocation may not be possible, the Privacy Officer must decide whether revocation is proper.
- d. **Conditions.** The Plan Sponsor, as an employer, can condition employment on the employee's authorizing the release of PHI from work-related medical services such as drug testing and fitness for duty physicals. The work-related conditions do not have to be in the Plan's policies and procedures.

#### D. **PROHIBITED USES AND DISCLOSURES**

1. **Underwriting Purposes.** The Plan will not use or disclose genetic information for underwriting purposes. Underwriting purposes does not include determinations of medical appropriateness where an individual seeks a benefit under the Plan, but means:
  - a. Rules for, or determination of, eligibility (including enrollment and continued eligibility) for, or determination of, benefits under the Plan  
  
(including changes in deductibles or other cost-sharing mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program).

- b. The computation of premium or contribution amounts under the Plan (including discounts, rebates, payments in kind, or other premium differential mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program).
  - c. The application of any pre-existing condition exclusion under the Plan.
  - d. Other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits.
2. **Sale of PHI.** The Plan will not sell PHI. Sale of PHI means a disclosure of PHI by the Plan where the Plan directly or indirectly receives remuneration from or on behalf of the recipient of the PHI in exchange for the PHI. Sale of PHI does not include a disclosure of PHI:
- a. For public health purposes pursuant to 45 C.F. R. §164.512(b) or §164.514(e).
  - b. For research purposes pursuant to 45 C.F.R. §164.512(i) or §164.514(e), where the only remuneration received by the Plan is a reasonable cost-based fee to cover the cost to prepare and transmit the PHI for such purposes.
  - c. For treatment and payment purposes pursuant to 45 C.F.R. §164.506(a).
  - d. For the sale, transfer, merger or consolidation of all or part of the Plan and for related due diligence pursuant to 45 C.F.R. §164.506(a).
  - e. To or by a Business Associate for activities that the Business Associate undertakes on behalf of the Plan, pursuant to 45 C.F.R. §164.502(e) and §164.504(e), and the only remuneration provided is by the Plan to the Business Associate for the performance of such activities.
  - f. To an individual when requested under 45 C.F.R. §164.524 or §164.528.
  - g. Required by law as permitted under 45 C.F.R. §164.512(a).
  - h. For any other purpose permitted by and in accordance with the applicable requirements of this Policy IV.D.2, where the only remuneration received by the Plan is a reasonable, cost-based fee to cover the cost to prepare and transmit the PHI for such purpose or a fee otherwise expressly permitted by other law.

V. **POLICY SUBJECT: USES AND DISCLOSURES PERMITTED FOR REASONS OTHER THAN TREATMENT, PAYMENT AND HEALTH CARE OPERATIONS WITHOUT INDIVIDUAL AUTHORIZATION.**

**POLICY:** In the following limited instances, the Plan will be permitted to use or disclose PHI without an individual's consent or authorization.

A. **USES AND DISCLOSURES THAT REQUIRE AN OPPORTUNITY FOR THE INDIVIDUAL TO AGREE OR TO OBJECT (45 C.F.R. §164.510)** (Applicable to Emergency situations.)

1. **Disclosures to Designated Individuals.** The Privacy Officer, without written consent or authorization from the individual, may authorize the use or disclosure of PHI to any person identified by the individual, such as a family member or close friend, of any PHI directly relevant to such person's involvement with the individual's health care or payment related to the individual's health care as long as the following conditions are met:

a. If the individual is present for, or otherwise available prior to, this type of use or disclosure and has the capacity to make health care decisions, the Privacy Officer will authorize the use or disclosure of the PHI if the Plan: (1) obtains the individual's authorization; (2) provides the individual with the opportunity to object and the individual does not do so; (having a written authorization is a waiver of this requirement).

(i) If written notification and agreement is not possible, the Privacy Officer may orally inform the individual and obtain oral agreement from the individual. If the exchange is oral, the Privacy Officer will document the exchange and maintain the documentation in accordance with 45 C.F.R. §164.530(j) and Policy XX.

2. **Disclosures for Notification Purposes.** The Privacy Officer, without written authorization or consent from the individual, may authorize the use or disclosure of PHI to notify, or assist in notifying (including identifying or locating), a family member, a personal representative of the individual, or another person responsible for the individual's care, of the individual's location, general condition or death. The Privacy Officer also may authorize the use or disclosure of PHI to a public or private entity that is authorized by law or by its charter to assist in disaster relief, for the purpose of coordinating with such entities to notify (including identifying or locating) relatives or those close to the individual, of the individual's location, general condition or death. The requirements specified above in V.A.1 are applicable unless the Privacy Officer determines those requirements interfere with efficient emergency response.

3. **Disclosures When the Individual is Deceased.** If the individual is deceased, the Privacy Officer may disclose to a family member, other relative, a close personal friend of the individual or any other persons identified by the individual who were involved in the individual's care or payment for health care prior to the individual's death, PHI of the individual that is relevant to such person's involvement, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the Privacy Officer.

**B. USES AND DISCLOSURES FOR WHICH AN INDIVIDUAL'S CONSENT, AUTHORIZATION OR OPPORTUNITY TO AGREE OR OBJECT ARE NOT REQUIRED. (45 C.F.R. §164.512)**

1. **Uses and Disclosures.** In the following circumstances, the Privacy Officer may authorize the use or disclosure of PHI without the individual's written consent or authorization, and without giving the individual the right to agree or object.
  - a. To the appropriate governmental or judicial authority as required by law in situations of abuse, neglect or domestic violence (45 C.F.R. §164.512(c)); in the course of any judicial or administrative proceeding (45.C.F.R. §164.512(e)); for law enforcement purposes to a law enforcement official as required by law (45 C.F.R. §164.512(f)). The Plan will only make such disclosures to the extent they are required by law and the use or disclosure complies with and is limited to the relevant requirements of the law. Further, in making such disclosures, the Plan will comply with the additional requirements in 45 C.F.R. §§164.512(c), (e), or (f), as applicable.
  - b. To the appropriate public health authority that is authorized by law to collect or receive PHI for the purpose of preventing or controlling disease (including notifying infected individuals when authorized by law), injury or disability; or to receive reports of child abuse or neglect (45 C.F.R. §164.512(b)(1)(i)- (ii), (iv)). The Plan will comply with the additional requirements in 45 C.F.R. §164.512(b)(1)(i)-(ii), (iv).
  - c. To persons or entities subject to the jurisdiction of the Food and Drug Administration ("FDA") to meet the reporting requirements of the FDA, such as submitting adverse event reports, tracking products for recalls, and conducting post-marketing surveillance to track compliance (45 C.F.R. §164.512(b)(1)(iii)). The Plan will comply with the additional requirements in 45 C.F.R. §164.512(b)(1)(iii).
  - d. To an employer to comply with OSHA and MSHA requirements related to medical surveillance and work related injuries, and to persons as authorized by workers' compensation laws (45 C.F.R. §164.512(b)(1)(v) and §164.512(l)). The Plan will comply with the additional requirements in 45 C.F.R. §164.512(b)(1)(v) and §164.512(l).

- e. To health oversight agencies for oversight activities authorized by law, e.g., fraud and abuse audits, investigations and inspections; licensure or disciplinary actions; and civil, administrative or criminal proceedings (45 C.F.R. §164.512(d)). The Plan will comply with the additional requirements in 45 C.F.R. §164.512(d).
  - f. To coroners and medical examiners, and funeral directors, the PHI which is necessary to permit those persons to carry out their duties consistent with applicable law (45 C.F.R. §164.512(g)). The Plan will comply with the additional requirements in 45 C.F.R. §164.512(g).
  - g. To organ procurement organizations for donation purposes (45 C.F.R. §164.512(h)). The Plan will comply with the additional requirements in 45 C.F.R. §164.512(h).
  - h. For research purposes, provided that an Institutional Review Board or privacy board (as described in the Privacy Rule) approves the waiver of individual authorization and the additional conditions in 45 C.F.R. §164.512(i) are met. The Plan will comply with the additional requirements in 45 C.F.R. §164.512(i).
  - i. To appropriate persons and consistent with applicable laws and standards of ethical conduct, when the Privacy Officer believes, in good faith, that it is necessary to use or disclose the PHI to prevent or lessen a serious and imminent threat to the health and safety of a person or the public, or to assist law enforcement in identifying or apprehending an individual (45 C.F.R. §164.512(j)). The Plan will comply with the additional requirements in 45 C.F.R. §164.512(j).
  - j. To military and veterans authorities, national security and intelligence sources, protective services for the President, correctional institutions and other custodial law enforcement, and Department of State for the purposes detailed in 45 C.F.R. §164.512(k)(1)-(5). The Plan will comply with the additional requirements in 45 C.F.R. §164.512(k)(1)-(5).
2. **Verification Procedures.** Before making any such disclosures, the Privacy Officer will verify the identity of the person requesting the PHI and the authority that person has to have access to the requested PHI. (45 C.F.R. §164.514(h)).

In the normal course, the Privacy Officer will obtain the requisite verification by requiring the requester to send their request in writing on official stationery, and by calling the requestor. The Privacy Officer may also require the requester to provide any other documentation that he/she deems necessary, using professional judgment, to verify the authenticity of the requester.

- a. If the request is made to the Privacy Officer in person, the Privacy Officer will require the requester to present sufficient official identification, such as a badge or official credential, to verify the requester's identity and authority.

- b. If the request is made pursuant to legal process, such as a subpoena, warrant or court order, the Privacy Officer may rely on the veracity of that request.
  - c. If the Privacy Officer determines, using professional judgment, that there is an emergency situation that does not allow for a written exchange, the Privacy Officer may verify the requester's identity by calling the requester back. If this occurs, the Privacy Officer must document the exchange and the nature of the emergency, and maintain the documentation in accordance with 45 C.F.R. §164.530(j) and Policy XX.
- C. **DISCLOSURES TO "BUSINESS ASSOCIATES" (45 C.F.R. §160.103).** The Plan may disclose PHI to "Business Associates" consistent with Policy VIII.
- D. **DISCLOSURES TO GROUP HEALTH PLAN SPONSOR OF PHI HELD BY GROUP HEALTH PLAN, HEALTH INSURANCE ISSUERS OR HMOs. (45 C.F.R. §164.504(f)).** The Plan will not disclose PHI held by it to the Plan Sponsor, unless and until the Plan Sponsor has amended the Plan documents to incorporate specific protective provisions, the Plan Sponsor has provided the Plan Administrator with a copy of the amended Plan documents, and the Plan Sponsor has provided the Plan Administrator with a certification that it has made the required Plan amendments.
- E. **DISCLOSURES BY WHISTLEBLOWERS AND PLAN SPONSOR EMPLOYEE CRIME VICTIMS.** The Plan Sponsor Employees will not be disciplined if they disclose PHI to a health oversight agency or to an attorney only if they believe, in good faith, that the Plan has engaged in unlawful conduct. If a Plan Sponsor Employee believes that he/she should disclose PHI about a suspected perpetrator of a criminal act to a law-enforcement official, if feasible, that workforce member should first discuss that disclosure with the Privacy Officer. See 45 C.F.R. §§164.512(f)(2)(i) and 164.502(j).

VI. **POLICY SUBJECT: THE MINIMUM NECESSARY REQUIREMENT**

**POLICY:** The Plan generally will apply the minimum necessary standard, as defined in 45 C.F.R. §164.502(b), whenever it uses or discloses PHI to a third party, or requests PHI from another covered entity. This means that the Plan will make reasonable efforts to limit the use or disclosure, or request of PHI to the minimum necessary to accomplish its intended purposes.

A. **APPLICABILITY OF THE MINIMUM NECESSARY REQUIREMENT.** The Plan will apply the minimum necessary standard to all uses and disclosures of PHI, except as follows:

1. Disclosures to or requests by a health care provider for treatment purposes;
2. Permitted and required disclosures to the individual who is the subject of the information;
3. Uses or disclosures pursuant to a valid authorization executed by the individual.
4. Disclosures made to the Secretary of HHS in accordance with the Privacy Rule.
5. Uses and disclosures required by law as described above in Policy .B.1.a.

B. **IDENTIFICATION OF PLAN SPONSOR EMPLOYEES**

1. **Identified Plan Sponsor Employees.** The Plan Sponsor Employees who need access to PHI are identified above in Policy II (Personnel Designations) and Policy III.B (Persons Authorized to Access PHI, defined as “Authorized Employees”). No other Plan Sponsor Employees shall have access to PHI unless specifically authorized in writing by the Privacy Officer.
2. **Restrictions on Authorized Employees’ Access.** Authorized Employees who need access to PHI only have access to the PHI necessary for their job duties, as expressly limited in Policy III.B. No Authorized Employee may have access to PHI beyond that specified in Policy III.B unless specifically authorized in writing by the Privacy Officer.

C. **MINIMUM NECESSARY REQUIREMENT APPLIED TO USES, DISCLOSURES AND REQUESTS OF PHI.**

1. **Routine Uses, Disclosures or Requests; Protocol.** The Plan makes the following routine uses, disclosures or requests of PHI, and the accompanying protocols ensure that the minimum necessary requirement has been met. The Authorized Employees who have access to the requested PHI will use and disclose this PHI in accordance with the below defined protocols.

- a. Use/Disclose: Claim, billing, utilization and payment information for purposes described in Policy III.B above.
    - b. Protocol: These uses, disclosures and requests are made in accordance with access controls described in Policy III.B. In addition, the Authorized Employees shall ensure that the minimum amount of PHI reasonably necessary to accomplish the purpose is used, disclosed or requested.
  2. **Non-Routine Uses/Disclosures/Requests.** For each use, disclosure or request not specified above, the following criteria must be applied to ensure that the minimum necessary requirement has been met.
    - a. Criteria: The Privacy Officer will handle the request for a non-routine disclosure of PHI. Before disclosing the PHI, the Privacy Officer will verify the identity of the requesting party; verify that the disclosure is limited in scope and permissible under the policies and procedures and documents all disclosures for periods of six years from the date of the disclosure.
  3. **Reliance.** The Authorized Employee and the Privacy Officer may rely on the judgment of the requesting party in determining the minimum amount of information to be disclosed if:
    - a. The request for PHI is made by another covered entity; or
    - b. A public official makes the request for PHI, and the official represents that the information requested is the minimum necessary for the stated purpose.
  4. **Resolving Disputes.** In the course of using or disclosing PHI, the Privacy Officer will be responsible for negotiating with the requesting party about the amount of PHI that needs to be disclosed to comply with the minimum necessary requirement. The Privacy Officer will always seek to limit the disclosure to the extent possible without impeding on the health care delivery process. If the parties cannot agree on the amount of information that is the minimum necessary, the Privacy Officer will make the final determination.
- D. **LIMITATION REGARDING USING, DISCLOSING OR REQUESTING ENTIRE MEDICAL RECORD.** For all uses, disclosures, or requests to which the minimum necessary requirements apply, the Plan will not use, disclose or request an entire medical record, except when the entire medical record is specifically justified, and the Plan has documented the specific justification.

## VII. POLICY SUBJECT: **DE-IDENTIFICATION POLICY**

**POLICY:** The Plan may use or disclose de-identified information, which is health information that does not identify an individual and is not PHI, without obtaining the individual's consent or authorization.  
45 C.F.R. §164.514(a)

A. **CREATION OF DE-IDENTIFIED INFORMATION.** The Plan may create, or direct a Business Associate to create, de-identified information pursuant to the following guidelines (45 C.F.R. §164.514(b)).

1. **Expert Method.** The Plan may designate an expert, who has the appropriate knowledge of and experience with statistical and scientific principles and methods for rendering information not individually identifiable and applies such principles and methods to:
  - a. Determine that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is subject of the information; and
  - b. Document the methods and results of the analysis that justify such determination; or
2. **Removal of Identifiers Methods.** The Plan may remove the following individual identifiers related to individuals, their relatives, household members and employers, and ensure, to the extent practicable, that the de-identified information could not be used alone or in combination with other information to identify the individual who is a subject of the information.
  - a. Names;
  - b. All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, that complies with the specifics in 45 C.F.R. §164.514(b)(2)(i)(B);
  - c. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
  - d. Telephone numbers, fax numbers, and e-mail addresses;
  - e. Social Security numbers, medical record numbers, health plan beneficiary numbers, and account numbers;
  - f. Certificate/license numbers, vehicle identifiers and serial numbers; including license plate numbers, and device identifiers and serial numbers;

- g. Web Universal Resource Locators (URLs), and Internet Protocol (IP) address numbers;
  - h. Biometric identifiers, including finger and voice prints, full face photographic images and any comparable images; and
  - i. Any other unique identifying number, characteristic, or code.
3. **Business Associates.** The Plan may also disclose PHI to a Business Associate for de-identification, whether or not the de-identified information is to be used by the Plan. 45 C.F.R §164.502(d)(1)

**VIII. POLICY SUBJECT: BUSINESS ASSOCIATE RELATIONSHIPS**

**POLICY:**

The Plan will ensure that its “Business Associates,” the entities that perform services for the Medical Benefits and receive, use or disclose PHI that belongs to the Plan in the course of providing such services, will protect the privacy of the PHI. After the Plan obtains satisfactory, contractual assurances that the Business Associates will protect the PHI and limit their use and disclosure of PHI, the Plan will disclose PHI to its Business Associates only to the extent necessary for the Business Associates to carry out their contractual duties.

In addition, after providing the required assurances, the Business Associates may create or receive PHI on behalf of the Plan. As it is anticipated that most of the PHI contained in an Individual’s Designated Record Set will be in the possession and control of a Business Associate the relevant Business Associate will be required to respond to individual requests to inspect, copy, amend PHI in their possession and control as well as to requests for confidential communications/alternative means of communication and/or accounting of disclosures of such PHI as is in their possession and control.

Business Associate Agreements that are entered between the Plan and a Business Associate will contain provisions requiring that the Business Associate perform its contractual duties in accordance with the Policies and Procedures (if applicable) and with the HIPAA Privacy Rule.

**A. APPLICABILITY.**

1. The Plan will enter into Business Associate Agreements with all of its Business Associates. A Business Associate is an entity or person who:
  - a. performs or assists in performing a Plan function or activity involving the use and disclosure of PHI (such as claims processing or administration; data analysis; underwriting; audits and others); or
  - b. provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation, or financial services, where the performance of such services involves giving the service provider access to PHI.

**B. PROCEDURE.**

**Each Business Associate Agreement will describe in detail the Business Associate's obligations and responsibilities regarding the use and/or disclosure of PHI.**

1. **Monitoring and Non-Compliance.** The Privacy Officer will monitor the Business Associate's compliance with these obligations to the extent that the Privacy Officer will investigate any credible evidence that Business Associate has violated the Business Associate agreement. Any Plan Sponsor Employee, Business Associate or agent who becomes aware that a Business Associate may be violating its obligations to the Plan, must immediately report such violation to the Privacy Officer, who must investigate the matter and, if warranted, take reasonable steps to end and cure the violation.
  - a. **Additional Measures.** If the reasonable steps taken are unsuccessful, the Plan will terminate the contract with the Business Associate, if feasible. If there are no other viable business alternatives, so that termination is not feasible, the Privacy Officer will promptly report the matter to the Department of HHS.
2. **Disclosures by Whistleblowers and Workforce Member Crime Victims.** The Plan will not terminate a Business Associate contract if the Business Associate discloses PHI to a health oversight agency or to an attorney because it believes, in good faith, that the Plan has engaged in unlawful conduct. 45 C.F.R. §164.512(f)(2)(i) and 164.502(j).

## VIII. POLICY SUBJECT: BREACHES OF UNSECURED PROTECTED HEALTH INFORMATION

**POLICY:** The Plan will investigate all potential breaches of unsecured PHI and notify affected participants, the Department of Health and Human Services and, if applicable, the media if a breach of unsecured PHI has occurred.

- A. **REPORTING REQUIREMENTS.** If any person, including a Plan Sponsor Employee or Business Associate’s employee, knows or suspects that PHI is used or disclosed in violation of HIPAA, the employee must notify the Privacy Officer. The employee must report an actual or suspected violation immediately, without waiting to verify facts.
- B. **INVESTIGATION.** The Privacy Officer will conduct an investigation and make a determination as to whether:
1. the PHI at issue is “secured” or “unsecured” as defined under HIPAA (45 C.F.R. §164.402);
  2. there has been an acquisition, use or disclosure of unsecured PHI in violation of HIPAA (45 C.F.R. §164.402);
  3. the HIPAA violation compromises the security or privacy of the PHI; and
  4. any exceptions apply that would relieve the Plan of the obligation to notify the individual whose PHI is at issue.

Unless an exception to the definition of a breach applies (45 C.F.R. §164.402(1)), an acquisition, access, use or disclosure of PHI in violation of HIPAA will be presumed to be a breach unless the Privacy Officer finds that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification.

The unauthorized person who used the PHI or to whom the disclosure was made.

Whether the PHI was actually acquired or viewed.

The extent to which the risk to the PHI has been mitigated.

If the Privacy Officer determines at any step of the investigation that the circumstances do not rise to the level of a “breach” (as defined by 45 C.F.R. §164.402) or that the Plan is not otherwise required to provide notice, the Privacy Officer shall stop the investigation, document the determination, and retain the documentation in the Plan’s HIPAA compliance files (see Policy XX).

C. **NOTIFICATION.** If a breach of unsecured PHI has occurred and no exceptions apply, the Privacy Officer shall prepare or oversee the preparation of appropriate notification. Such notification shall include:

1. a description of the circumstances of the breach, including the date of the incident and the date the incident was discovered;
2. a description of the types of PHI involved in the breach;
3. any steps the individual should take to protect himself or herself from potential harm;
4. a description of what steps the Plan is taking to investigate the breach, mitigate harm, and protect against any further breaches; and
5. contact information and procedures to be used if the individual has questions about the notification.

The notification will be prepared and sent to affected individuals as soon as reasonably possible and without unreasonable delay, but in no case more than 60 calendar days after the breach is, or should have been, discovered. The Privacy Officer will also provide or oversee provision of timely notice to the Department of Health and Human Services and prominent media outlets, if and in the manner required by HIPAA (45 C.F.R. §§164.406 and 164.408).

IX. **POLICY SUBJECT: REQUESTS TO RESTRICT USES AND DISCLOSURES**

**POLICY:** Individuals may request that restrictions or limitations be placed on the use or disclosure of their PHI by the Plan as described below.

A. **PARAMETERS OF REQUESTED RESTRICTIONS.**

1. Individuals may request that restrictions be placed on the PHI that the Plan may use or disclose for treatment, payment or health care operations.
  - a. For example, in situations of a separation or divorce, where the Guardian parent wants to limit access of PHI to the other parent.
2. Individuals also have the right to request a limit on the PHI that the Plan discloses to a third party involved with the individual's care or payment for care rendered.
3. An agreed upon restriction may not prevent uses or disclosures of PHI that are permitted or required by the Privacy Rule. 45 C.F.R. §164.522(a)(1)(v).

B. **THE PLAN IS NOT REQUIRED TO AGREE TO REQUEST.**

1. The Plan is **not required to agree** to a request.
2. If the Plan agrees to a documented restriction, the Plan will abide by that agreement, except in cases of an emergency. (45 C.F.R. §164.522(a)(1)(iii) and (iv)). The Privacy Officer will notify the appropriate Business Associates of the agreed upon restrictions. If the individual who requested the restriction is in need of emergency treatment and the restricted PHI is needed to provide emergency treatment, the Plan may use the restricted PHI or may disclose such information to a health care provider to provide such treatment to the individual. If the Plan discloses restricted PHI to a health care provider for emergency treatment, the Plan must request that such health care provider not further use or disclose the information.

**IMPORTANT: UNLESS THERE IS AN EMERGENCY, ALL QUESTIONS AS TO THE APPLICATION OF THESE PROVISIONS MUST BE REFERRED TO THE PRIVACY OFFICER BEFORE ANY DISCLOSURE OR REQUEST IS MADE.**

C. **TERMINATING RESTRICTIONS.**

A restriction may be terminated if (45 C.F.R §164.522(a)(2)):

1. The individual agrees to or requests the termination in writing;
2. The individual agrees orally to the termination and the oral agreement is documented by the Plan; or
3. The Plan informs the individual that it is terminating its agreement to a restriction, except that such termination is only effective with respect to PHI created or received after the individual has been informed.

- D. **DOCUMENTATION.** All information related to an individual's request for a restriction as described herein must be retained for six (6) years in accordance with 45 C.F.R. §164.530(j) and Policy XX.

X. **POLICY SUBJECT: REQUESTS BY INDIVIDUALS TO INSPECT AND COPY THE DESIGNATED RECORD SET (DRS)**

**POLICY:** Individuals have a right to inspect and copy part or all of their DRS. As most of an individual's DRS is in the possession and control of Business Associates of the Plan, individuals will be directed to address their request as stated in the following procedure:

A. **PROCEDURE** (45 C.F.R. §164.524(b)).

1. **Written Request.** To inspect and copy any part of the DRS, an individual must submit a request in writing as follows:

a. If regarding access to medical benefit payment or claims adjudication information, to:

**Florida Blue, by contacting  
the customer service  
number on the individual's  
ID card**

b. If regarding access to dental benefit payment or claims adjudication information, to:

**Brown & Brown PRIA  
Attn: Robin Riley, Account Executive  
PO Box 2416, Daytona Beach, FL 32115  
386-239-4051 phone / 386-845-9229 fax  
rriley@bbpria.com**

c. If regarding [medical and/or dental] enrollment information to:

**Public Risk Management of Florida  
Attn: Doris Bernard  
3434 Hancock Bridge Parkway, Suite 203  
Fort Myers, FL 33903  
239-599-4824 phone / 239-656-1066 fax  
dbernard@prm-fl.com**

d. If regarding payment and claims adjudication for vision services, to:

**VSP (Vision Service Plan)  
by contacting 1-800-877-7195**

e. If regarding records, payment and claim adjudication information under the Employee Assistance Program to:

**MHNet Behavioral Health  
by contacting 1-800-272-3626**

f. An individual may also submit any request for their DRS to the Privacy Officer who will forward the request to the appropriate Business Associate for action. For requests pertaining to PHI dated prior to January 1, 2002, the Privacy Officer will take all appropriate and reasonable steps to provide the requested PHI.

f. All requests will be in writing and must state:

The purpose: inspection and/or copying;

- The individual's name, address, date of birth and Employer name and location;
- A description of the PHI the individual is seeking; and
- If the individual's request for access directs the Plan to transmit the copy of PHI directly to another person designated by the individual, the individual's signature, clear identification of the designated person and where to send the copy of the PHI.

2. **Required Information.** The designated record set to which the individual will be entitled includes,

- a. Subject to section C.1 of this Policy, any PHI, (such as enrollment, payment, claims adjudication records, or any PHI used to make coverage decisions) that is in the possession of the Plan Sponsor Employees or a Business Associate.
- b. The Plan may deny individual access to PHI as described in section C.1 of this Policy.

3. **Time for Response/Access.** Except as provided below, any request for access will be responded to by the Privacy Officer or Associate Privacy Officer or the appropriate Business Associate no later than 30 days after it was received. (45 C.F.R. §164.524(b)(2)). A one-time extension of 30 days is available to the Plan or Business Associate if it is unable to take action within the first 30 days. Within the first 30 days after the individual's request is made, individual will be furnished with a written statement that states:

- a. The reasons for the delay and;
- b. The date by which a response will be provided.

## B. GRANTING OF REQUEST.

1. **Procedure.** If a request for access to PHI made directly to the Privacy Officer is granted by the Plan, the Privacy Officer or the Business Associate the request has been forwarded to, will notify the requesting party in writing of the acceptance of the request and the requested access will be provided. (45 C.F.R. §164.524(b)(2)(i)(A))

2. **Access.** The access will include inspection, copying or both and the Privacy Officer will (45 C.F.R. §164.524(c)):

- a. Arrange with the individual for a convenient time and place to inspect or obtain a copy of the PHI;
- b. Mail the PHI to the individual at his/her request; or
- c. If an individual's request for access directs the Plan to transmit the copy of the PHI directly to another person designated by the individual, the Plan will provide the copy to the person designated by the individual.

3 **PHI Maintained by Business Associates.** The Plan will ensure that any PHI related to the individual that is maintained by one of the Plan's Business Associates will be made available to said individual as part of his/her designated record set.

4 **Format.** The requested information will be provided in the form and format requested by the individual, unless it is not readily producible in such form or format. If the requested form or format cannot be provided, a readable hard copy form as agreed to by the Plan and the individual will be provided. If the requested PHI is maintained in more than one record set, that PHI need only be produced once.

If the PHI that is the subject of a request for access is maintained in one or more designated record sets electronically and if the individual requests an electronic copy of such information, the Plan or the Business Associate the request has been forwarded to will provide the individual with access to the PHI in the electronic form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by the Plan and the individual.

5 **Fees.** An individual may be charged a reasonable cost-based fee by the Plan for the labor for copying and preparation of an explanation or summary of the requested PHI, whether in paper or electronic form. The fee will include only the cost of (45 C.F.R. §164.524(c)(4)):

- (i) Labor for copying the PHI, whether in paper or electronic form;
- (ii) Supplies for creating the paper copy or electronic media if the individual requests that the electronic copy be provided on portable media;
- (iii) Postage when the individual requests mailing; and/or
- (iv) Preparation of the explanation or summary.

C. **DENIAL OF REQUEST FOR ACCESS.** A request to inspect and copy PHI may be denied in certain limited circumstances specified by the Privacy Rule. Florida Blue has retained the authority to determine denials for medical and prescription claims. All other Business Associates must obtain prior approval of the Privacy Officer before a decision to deny is taken and communicated to the individual.

1. **Requests That May Be Denied.** Requests for access to the following information may be denied (45 C.F.R. §164.524(a)):

- a. Psychotherapy notes (they are not part of the medical record);

- b. Information compiled in reasonable anticipation of, or use in, a civil, criminal or administrative action or proceeding;
- c. PHI maintained by the Plan that is subject to or exempted from the Clinical Laboratory Improvements Amendments of 1988 (CLIA);
- d. Information that a licensed healthcare provider has determined that access to may endanger the life or physical safety of the individual or other person;
- d. PHI that makes reference to another person, who is not a health care provider, and a licensed health care professional has determined that the access requested is reasonably likely to cause substantial harm to the other person;
- f. Access requested is made by the individual's personal representative and a licensed health care professional has determined that access to the personal representative is reasonably likely to cause substantial harm to the individual or another person;
- g. The individual agreed to temporary denial of access when he/she consented to participate in research that includes treatment, and the research is not yet complete. The individual's right of access will be reinstated upon completion of the research.
- h. The records are subject to the Privacy Act of 1974 and the denial of access meets the requirements of that law;
- i. The PHI was obtained from someone other than a health care provider under a promise of confidentiality and access would likely reveal the source of the information.

2. **Form of Denial.** A denial of a request for access must (45 C.F.R. §164.524(d)):

- a. Be written in plain language;
- b. State the basis for the denial;
- c. If applicable, state the individual's right to an independent review of the denial;
- d. If applicable, provide a description of how the individual may exercise such review rights; and
- e. Provide a description of how the individual may appeal the denial to the Plan or to the Secretary of HHS, including the name, title and telephone number of the Privacy Officer.

3. **Making Other Information Accessible.**

- a. **Partial Denial.** If access is denied, in part, the individual will be given access to any other PHI requested, after excluding the PHI for which access has been denied.

- b. **PHI Maintained by Other Entity.** If access is denied, in whole or in part, because the requested information is not maintained by the Plan, and the Plan knows where the requested information is maintained, the Privacy Officer will inform the individual where to direct the request for access.

**D. REVIEW OF DENIAL OF ACCESS.**

- 1. **Right of Review.** In certain instances, an individual whose request for access is denied has the right to have the denial reviewed by a licensed health care professional designated by the Plan who did not participate in the original decision. In other situations, the Plan may deny an individual access without providing an opportunity for review.
- 2. **Written Request For Review.** To secure review of a denial of a request to inspect and copy PHI, an individual must submit a request in writing to:

**Privacy Officer  
Jacqueline Martin, Human Resource Manager  
Levy County Commission, PO Box 310, Bronson FL 32621\**

- E. **DOCUMENTATION.** Information related to individual requests for access to their PHI and the titles of the Plan Sponsor Employees responsible for receiving and processing requests for access by individuals will be retained for six (6) years in accordance with 45 C.F.R. §164.530(j) and Policy XX.

XI. **POLICY SUBJECT: REQUESTS FOR CONFIDENTIAL COMMUNICATIONS OF PHI AND/OR ALTERNATIVE MEANS**

**POLICY:** Individuals may request that the Plan provide them with their PHI by confidential communications or at an alternative location as described below.

A. **STANDARD TO RECEIVE CONFIDENTIAL COMMUNICATIONS.** The Plan will accommodate an individual's reasonable request to receive communications of PHI in a confidential manner or at an alternative location. If the individual clearly and reasonably states that the disclosure of all or part of that information could endanger the individual, the Plan will accommodate the individual's request.

1. **Written Request.** For confidential communications or communications at an alternative location, an individual must make a request in writing to:

a. If regarding access to medical benefit payment or claims adjudication information, to:

**Florida Blue, by contacting  
the customer service number  
on the individual's ID card**

b. If regarding access to dental benefit payment or claims adjudication information, to:

**Brown & Brown PRIA  
Attn: Robin Riley, Account Executive  
PO Box 2416, Daytona Beach, FL 32115  
386-239-4051 phone / 386-845-9229 fax  
rriley@bbpria.com**

c. If regarding enrollment information for [medical and/or dental] benefits, to:

**Public Risk Management of Florida  
Attn: Doris Bernard  
3434 Hancock Bridge Parkway, Suite 203  
Fort Myers, FL 33903  
239-599-4824 phone / 239-656-1066 fax**

- d. If regarding payment and claims adjudication for vision services, to:

**NVA (National Vision Administrators, L.L.C.)  
by contacting 1-800-672-7723**

- e. If regarding records, payment and claim adjudication information under the Employee Assistance Program, to:

**MHNet Behavioral Health  
by contacting 1-800-272-3626**

- 2. **Required Information.** The request should specify how or where communications are to be made and a statement that disclosure of all or part of the information to which the request pertains could endanger the individual.
- 3. **Granting Requests.** The Plan will accommodate reasonable requests and may condition its accommodation on:
  - a. Information as to how payment, if any, will be handled and;
  - b. Specification of an alternative address or other method of contact.

- B. **DOCUMENTATION.** The Plan will maintain all information related to requests for confidential communications or communications at an alternative location for six (6) years as required by 45 C.F.R. §164.510(b) and 164.530(j) and Policy XX.

XII. **POLICY SUBJECT: ACCOUNTING OF DISCLOSURES OF PHI**

**POLICY:** Individuals have a right to receive an accounting from the Plan that lists certain disclosures of their PHI made by the Plan during the 6-year period prior to the request, but starting from April 14, 2003 (45 C.F.R. §164.528(a)). **Among the exceptions, disclosures of PHI purposes of treatment, payment or healthcare operations do not need to be accounted for.**

A. **PROCEDURES TO REQUEST AN ACCOUNTING.**

1. **Request for Accounting.** All requests for an accounting of disclosures must be submitted in writing to:

a. If regarding access to medical benefit payment or claims adjudication information, to:

**Florida Blue, by contacting  
the customer service number  
on the individual's ID card**

b. If regarding access to dental benefit payment or claims adjudication information, to:

**Brown and Brown PRIA  
Attn: Robin Riley, Account Executive  
PO Box 2416, Daytona Beach, FL 32115  
386-239-4051 phone / 386-845-9229 fax  
rriley@bbpria.com**

c. If regarding enrollment information for medical, dental, FSA, EAP and vision benefits, to:

**Levy County Commission  
Human Resource Office  
352-486-5219 phone  
352-486-5167 fax**

d. If regarding payment and claims adjudication for vision services, to:

**VSP**  
**by contacting 1-800-877-7195**

e. If regarding records, payment and claim adjudication information under the Employee Assistance Program to:

**MHNet Behavioral Health**  
**by contacting 1-800-272-3626**

f. Or to the attention of the Associate Privacy Officer at:

**Levy County Commission**  
**Human Resource Office**  
**352-486-5219 phone**  
**352-486-5167 fax**

2. **Required Information.** The individual's written request must state:
- a. Name, address and telephone number of person who is the subject of the information for which an accounting is requested;
  - b. Date of Birth and Participating Employer name;
  - c. Time period for which accounting is sought -- not to exceed 6 years from the date of the request; and
  - d. Format of the information sought -- paper or electronic (if electronic, requesting party must provide an e-mail address).
3. **Fees.** A single accounting request within a 12-month period will be free of charge. A requesting party will be responsible for paying a reasonable cost-based fee for any additional accounting requests, provided they are notified of the costs involved before they are assessed and given an opportunity to withdraw or modify the request.
4. **Time for Response/Access.** Except as stated, any request for an accounting will be acted upon no later than 60 days after it was received. (45 C.F. R. §164.528(c))
- a. A one-time extension of 30 days is available to the Plan if it is unable to take action within the first 60 days, provided that within the first 60 days the Plan provides the individual with a written statement stating:
    - (i) The reasons for the delay and;
    - (ii) The date by which a response will be provided.

**B. CONTENTS OF THE ACCOUNTING:**

1. **Accounting Requirements.** The accounting will be written and provide the following information to the individual: (45 C.F.R. §164.528(b)):
  - a. A list of the covered disclosures that occurred during the 6 years preceding the request, unless that period is shortened by the compliance date or the individual's request, and the date of each disclosure;
  - b. A list of the disclosures to or by Business Associates that occurred during the relevant time frame, and the date of each disclosure;
  - c. The name of the person or entity who received the disclosed information and, if known, the address of such person or entity;
  - d. A brief description of the PHI disclosed in each disclosure; and
  - e. A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis of the disclosure. In lieu of such statement, the Plan may provide a copy of a written request for a disclosure for the purpose of complying with the Secretary of HHS's compliance activities or for disclosures for which authorization is not required.
  
2. **Items Excluded.** The accounting for disclosures will **not** include the following disclosures:
  - a. Disclosures for carrying out treatment, payment or health care operations;
  - b. Disclosures pursuant to a valid authorization executed by the individual;
  - c. Disclosures of their PHI to the individuals;
  - d. Disclosures for the facilities directory, disclosures to persons involved in the individual's care, or for other notification purposes;
  - e. Disclosures for national security or intelligence purposes;
  - f. Disclosures to correctional institutions or law enforcement officials; or
  - g. Disclosures that occurred before April 14, 2003.
  
3. **Accounting Requirements; Multiple Disclosures.** If, during the period covered by the accounting request, the Plan has made multiple disclosures of PHI to the same person or entity for the purpose of complying with the Secretary of HHS's compliance activities or for disclosures for which authorization is not required or pursuant to a single authorization, the accounting may, with respect to such disclosures, provide (45 C.F.R. §164.528(b)(3)):
  - a. The information required by Section B.1 above for the first disclosure during the accounting period;
  - b. The frequency, periodicity, or number of disclosures made during the accounting period; and

- c. The date of the last such disclosure during the accounting period.

**C. SUSPENSION OF RIGHT.**

1. **Temporary Suspension of Right Through Written Request.** The Plan will temporarily suspend an individual's right to receive an accounting of disclosures pursuant to a health oversight agency or law enforcement official's request if the agency or official provides a written statement to the Plan. (45 C.F.R. §164.528(a)(2)(i)):
  - a. Stating that the accounting to the individual would likely impede the agency's activities and;
  - b. Specifying the time period for which the suspension is required.
  
2. **Temporary Suspension of Right Through an Oral Request.** If the agency or official statement requesting that an accounting not be disclosed is made orally, the Privacy Officer will (45 C.F.R. §164.528(a)(2)(ii)):
  - a. Document the statement, including the identity of the agency or official making the statement;
  - b. Temporarily suspend the individual's right to an accounting subject to the statement; and
  - c. Limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement as required above is submitted during that time.

- D. DOCUMENTATION.** Information related to any accountings of disclosures and the titles of the Plan's personnel responsible for receiving and processing requests for accountings will be retained for six (6) years in accordance with 45 C.F.R. §§164.530(j) and 164.528(a) and Policy XX.

XIII. POLICY SUBJECT: **AMENDMENT REQUESTS**

**POLICY:**

An individual has the right to request that the Plan amend his/her PHI or a record about the individual in a designated record set while the PHI is maintained in the designated record set. However, in certain instances described below, the Plan may deny the request (45 C.F.R. §164.526(a)). Florida Blue has the authority to determine a denial of amendment for medical and prescription drug coverage. Individuals must refer directly to the appropriate Business Associate. Other Business Associates must obtain the Plan's approval of a denial of amendment.

A. **AMENDMENT REQUEST PROCEDURE.**

1. **Amendment Requests.** All requests for amendments must be submitted in writing to:

a. If regarding access to Medical Benefit payment or claims adjudication information, to:

**Florida Blue, by contacting  
the customer service number  
on the individual's ID card**

b. If regarding access to dental benefit payment or claims adjudication information, to:

**Brown & Brown PRIA  
Attn: Robin Riley, Account Executive  
PO Box 2416, Daytona Beach, FL 32115  
386-239-4051 phone / 386-845-9229 fax  
rriley@bbpria.com**

c. If regarding enrollment information for [medical and/or dental] benefits to:

**Levy County Commissioners Office  
Attn: Human Resources  
PO Box 310  
Bronson, FL 32621  
352-486-5219 phone / 352-486-5167 fax  
martin-jacqueline@levycounty.org**

- d. If regarding payment and claims adjudication for vision services, to:

**VSP**  
**by contacting 1-800-877-7195**

- e. If regarding records, payment and claim adjudication information under the Employee Assistance Program to:

**MHNet Behavioral Health**  
**by contacting 1-800-272-3626**

- g. Or to the attention of the Privacy Officer at:

**Human Resource Manager**  
**Levy County Commission**  
**PO Box 310, Bronson, FL 32621**  
**352-486-5219 phone**  
**[martin-jacqueline@levycounty.org](mailto:martin-jacqueline@levycounty.org)**

- 2. **Required Information.** The written request should state:

- a. Name, address and telephone number of person who is the subject of the information for which an amendment is requested;
- b. Date of Birth and Participating Employer;
- c. The reason(s) in support of the request.

- 3. **Time for Action on Notice of an Amendment.** Amendment requests will be acted upon no later than 60 days after receipt of the request. (45 C.F.R. §164.526(b)(2))

- a. A one-time 30-day extension is available to the Plan so long as the individual is provided, within the time limit stated in Section 3 above, with a written statement of:
  - (i) The reasons for the delay; and
  - (ii) The date by which the Plan will complete the requested amendment.

- B. **GRANTING AN AMENDMENT REQUEST.** If the Plan grants the request, in whole or part, it will (45 C.F.R. §164.526(c)):

- 1. Make the appropriate amendment to the PHI or record that is the subject of the request by, at a minimum, identifying the records in the designated record set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment;

2. Timely inform the individual that the amendment is accepted and obtain the individual's identification of, and agreement to have the Plan notify the relevant persons with which the amendment needs to be shared; and
3. Make efforts to inform and provide, within a reasonable time, the amendment to:
  - a. Persons identified by the individual as having received PHI about the individual and needing the amendment; and
  - b. Persons, including Business Associates, that the Plan knows have the PHI that is the subject of the amendment and that may have relied, or could foreseeably rely, on such information to the detriment of the individual.

**C. DENIAL OF AN AMENDMENT REQUEST (45 C.F. R. §164.526(a)(2) and (b)).**

1. **Reasons for Denial.** The Plan may deny a request for amendment for the following reasons:
  - a. It is not in writing;
  - b. It does not include a reason to support the request;
  - c. The information was not created by the Plan, unless the individual shows that the originator of the PHI is no longer available to make the amendment;
  - d. The information is not PHI kept by or for the Plan;
  - e. The information is not part of the information the individual would be permitted to inspect and copy as set forth herein at Policy X (45 C.F.R. §164.524); or
  - f. The information that the individual seeks to amend is accurate and complete.
  
2. **Timely, Written Denial.** A denial will be in writing and state in plain language (45 C.F.R. §164.524(d)):
  - (i) The basis for denying the amendment;
  - (ii) The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement;
  - (iii) That if the individual does not submit a statement of disagreement, he/she may request that his/her request for amendment and denial be provided with any future disclosures of the PHI that is the subject of the amendment request;
  - (iv) A description of the Plan's complaint procedure, including the name or title and telephone number of the Privacy Officer; and
  - (v) A description of how to appeal the denial to the Secretary of HHS.

**D. DISAGREEMENT AND REBUTTAL PROCEDURE.**

1. **Statement of Disagreement and Rebuttal.** In the event that an individual files with the Plan a statement of disagreement, as he/she is entitled to do, the Privacy Officer may include a written rebuttal to the individual's statement of disagreement. (45 C.F.R. §164.526(d)(3)). If a rebuttal is prepared, a copy will be provided to the individual.
2. **Appending to the Record.** The Privacy Officer must identify the record of PHI and the record that is the subject of the disputed amendment and append or otherwise link the following to the designated record set (45 C.F.R. §164.526(d)(4)):
  - a. The individual's amendment request;
  - b. The denial;
  - c. The individual's statement of disagreement, if any; and
  - d. The rebuttal, if any.
3. **Future Disclosures.** The following materials will be included with an individual's PHI when disclosed: (45 C.F. R. §164.526(d)(5))
  - a. **Where Statement of Disagreement Filed.** If the individual has submitted a statement of disagreement, the Plan will include with any subsequent disclosure of the PHI to which the disagreement relates, the material appended in accordance with Section 2 above or an accurate summary of any such information.
  - b. **Where No Statement of Disagreement Filed.** If the individual has not submitted a written statement of disagreement, the Plan will include the individual's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of PHI only if the individual has requested such action. (See 45 C.F.R. §164.526(d)(5)(ii)).

- c. **Notice of Amendment by Other Entity.** In the event that the Plan is informed by another covered entity of an amendment to an individual's PHI, it must amend the PHI in designated record sets in accordance with Section B above. (45 C.F.R. §164.526(e))

- E. **DOCUMENTATION.** Information related to any request for an amendment to PHI and the titles of the Plan Sponsor Employees who are responsible for receiving and processing requests for amendment will be retained for six (6) years in accordance with 45 C.F.R. §164.530(j) and Policy XX.

## XIV. POLICY SUBJECT: COMPLAINTS

**POLICY:** All individuals who are covered participants of the Plan (including dependents) who believe their privacy rights have been violated or who have a complaint arising under the Privacy Rule or these policies and procedures have the right to make an inquiry or complaint with the Privacy Officer or with the Secretary of Health and Human Services. (45 C.F.R. §164.530(d)(1))

### A. PROCEDURE.

1. **Reporting.** Individuals may make a report/complaint as follows:

- a. An individual must make a complaint in writing to the Privacy Officer, or to the HHS. The Privacy Officer is available to discuss any questions the individual might have about the complaint procedure.

An individual may contact the Privacy Officer at the following address/phone number:

**Human Resource Manager  
Levy County Commission  
PO Box 310, Bronson, FL 32621  
352-486-5219 phone  
martin-jacqueline@levycounty.org**

2. **Investigation.** When an individual submits a complaint, the Privacy Officer will investigate the circumstances related to the complaint.

- a. Reasonable Steps. The Privacy Officer may take the following steps, as he/she deems appropriate, to investigate the alleged violation: interview the complainant; interview the Authorized Employees or Business Associates who may have knowledge of the alleged violation; and review any relevant documents that pertain to the alleged violation. These procedures are not exclusive and the Privacy Officer may take any additional steps he/she deems necessary to investigate the complaint. Confidentiality will be maintained throughout the investigative process to the extent practicable and consistent with the need to undertake a full investigation.
- b. Results of Investigation. If the Privacy Officer determines that a violation in fact occurred, appropriate action will be taken as is necessary and supported by the facts, including:
  - (i) Disciplining Plan Sponsor Employees who have acted improperly, and ensuring any Business Associate employees who have acted improperly are disciplined by the Business Associate;
  - (ii) Working with a Business Associate to cure any violation by the Business Associate, or terminating the Business Associate contract if no cure is possible;

(iii) Mitigating any harmful effect that the Plan Sponsor Employees know of resulting from the improper use or disclosure of PHI as per Policy XV.

3. **Determination.** Upon completion of the investigation, appropriate action will be taken, if necessary and supported by the facts.
4. **Documentation.** Information related to each complaint received and the disposition of each complaint will be documented by the Plan, and that documentation will be retained for six (6) years, in accordance with §164.530(j) and Policy XX.

**XV. POLICY SUBJECT: MITIGATION**

**POLICY:** The Plan, to the extent practicable, will mitigate any harmful effect that it knows of resulting from the use or disclosure of PHI in violation of these policies and procedures or the Privacy Rule by the Plan, any of its Plan Sponsor employees or Business Associates.  
45 C.F.R. §164.530(f)

**A. REPORTING REQUIREMENTS.** Any person, including a Plan Sponsor Employee or Business Associate's employee, who becomes aware that an improper disclosure was made must immediately:

1. Limit any further improper disclosure; and
2. Report the matter to the Privacy Officer.

**B. MITIGATION STRATEGY.**

1. **Process.** In order to mitigate any harmful effects of an improper use or disclosure that the Plan knows of, the Privacy Officer may take the following steps:
  - a. Notify the affected individual;
  - b. Immediately request the return or destruction of the PHI by the disclosing party or the party who received the PHI;
  - c. Create additional safeguards for protecting PHI;
  - d. Discipline Plan Sponsor Employees who have acted improperly;
  - e. Work with the Business Associate to cure a violation, including requesting that the Business Associate discipline any involved employees; and
  - f. Terminate a Business Associate contract if the violation does not cease and it is practicable; or in the alternative, if it is not feasible to terminate the Business Associate contract, report the violation to the Secretary of the HHS.

The foregoing steps are not mandatory or exclusive and the Privacy Officer may take any steps he deems necessary to mitigate the violation.

XVI. **POLICY SUBJECT: NON-RETALIATION**

**POLICY:** The Plan, the Plan Sponsor Employees and the Business Associates are prohibited from intimidating, threatening, coercing, discriminating against or taking any retaliatory action against any individual for exercising his/her rights under the Privacy Rule or these policies and procedures. (45 C.F.R. §164.530(g)).

- A. **PROHIBITED RETALIATORY ACTIONS.** The Plan, the Plan Sponsor Employees, and the Business Associates will not retaliate against any individual because he/she in good faith:
1. Exercised any right under, or participated in any process established by, these policies and procedures or the Privacy Rule;
  2. Filed a complaint with the Privacy Officer or Secretary of HHS;
  3. Testified, assisted or participated in an investigation, compliance review, proceeding, or hearing conducted by the Secretary of HHS; or
  4. Opposed any act or practice made unlawful by the Privacy Rule or improper by these policies and procedures, provided that the individual or person has a good faith belief that the practice opposed is unlawful or contrary to these policies and procedures, and the manner of the opposition is reasonable and does not involve an impermissible disclosure of PHI.
- B. **PROCEDURE.** The report and investigation of allegations of retaliation will follow the procedures set forth in Policy XIV (Complaints).
- C. **SANCTIONS.** Any workforce member found to have retaliated against an individual for making a complaint under Policy XIV or for participating in an investigation will be subject to appropriate sanctions as set out in Policy XIX. Any Business Associate employee found to have retaliated against an individual will be sanctioned in accordance with the Business Associate's sanctions policies.

## **XVII. POLICY SUBJECT: TRAINING**

**POLICY:** The Plan will train all Authorized Employees on these policies and procedures with respect to PHI as required by the Privacy Rule as necessary and appropriate for said Authorized Employees to carry out their functions. (45 C.F.R. §164.530(b)(1) and (2))

### **A. TRAINING REQUIREMENTS.**

1. **Responsibility.** The Privacy Officer is responsible for ensuring timely and proper training.
2. **Time for Training.** Training will be provided:
  - a. To each Authorized Employee no later than April 14, 2003 or as soon thereafter as practicable. After April 14, 2003, no Authorized Employee will be authorized to handle PHI unless trained appropriately;
  - b. To each new Authorized Employee within a reasonable time after joining the workforce; and
  - c. To Authorized Employees whose functions are affected by material changes in policies or procedures within a reasonable time after the effective date of those changes. (45 C.F.R. §164.530(b)(2))

**B. DOCUMENTATION.** The Privacy Officer will document that all training has been provided as required and retain those records for six (6) years in accordance with 45 C.F.R. §164.530(j) and Policy XX. Such training may be documented through documents such as training rosters that show the dates of training, the subject of the training, the name and signature of attendees.

## XVIII. POLICY SUBJECT: NOTICE OF PRIVACY PRACTICES; DISSEMINATION; CHANGES

**POLICY:** The Plan will disseminate and maintain a Notice of Privacy Practices (“Privacy Notice”) that clearly states the manner in which it may use and disclose the individuals’ PHI, and provides adequate notice of the individuals’ rights and the Plan’s legal duties with respect to PHI. Individuals have a right to request and receive a paper copy of the Privacy Notice at any time. (45 C.F.R. §164.520(a))

### A. **PRIVACY NOTICE.** (45 C.F.R. §164.520(b))

1. **Responsibility.** The Privacy Officer is responsible for developing, reviewing, revising, updating and disseminating the Plan’s Privacy Notice to ensure that it conforms to these policies and procedures.
2. **Reservation of Rights to Change Policy/Notice.** The Plan, acting through the Plan Administrator or the Privacy Officer, reserves its right to revise these policies and procedures and any other related documentation, such as the Privacy Notice, at any time for any reason. Any such revisions may be effective for PHI currently in its possession as well as any information it receives in the future.
  - a. **Changes to Comply with Law:** These policies and procedures will be changed to maintain compliance with the Privacy Rule and/or governing law.
  - b. **Corresponding Changes to Privacy Notice:** If there is a change in these policies and procedures a corresponding change will be made to the Privacy Notice to comply with the notice requirements of the Privacy Rule.
3. **Change to Term Covered by Privacy Notice.** The Plan may change a privacy practice that is described in the Privacy Notice, and the related policies and procedures, without having reserved the right to do so, provided that such change (45 C.F.R. §164.530(i)):
  - a. Is effective only with respect to PHI created or received after the effective date of the Privacy Notice;
  - b. Complies with the Privacy Rule;
  - c. Is documented in accordance with 45 C.F.R. §164.530(j); and
  - d. Is incorporated into a revised Privacy Notice that is made available as required by the Privacy Rule and these provisions. (45 C.F.R. §164.520(c))

4. **Change to Term Not Covered by Privacy Notice.** The Plan may change, at any time, a policy or procedure that does not materially affect the content of the Privacy Notice, provided that:
  - a. The policy or procedure, as revised, complies with the Privacy Rule and these provisions; and
  - b. Prior to the effective date of the change, the policy or procedure, as revised, is documented in accordance with 45 C.F.R. §164.530(j) and Policy XX.

**B. DISSEMINATION OF PRIVACY NOTICE.**

1. **Time to Notify Individuals.** The Privacy Notice must be available on request to any person and/or individual as follows:
  - a. **Notification by the Plan.** The Plan must distribute the “Notice of Privacy Practices” as follows: (45 C.F.R. §164.520(c)(1))
    - (i) To participants covered by the Plan by April 14, 2003 via US Mail;
    - (ii) At enrollment for new enrollees in new hire packets supplied by **Human Resources/Risk Management/Benefits**; and
    - (iii) If there is a material change to the Privacy Notice, the change or the revised Privacy Notice will be prominently posted at [levycounty.org](http://levycounty.org) website by the effective date of the material change to the Privacy Notice, and in the Plan’s next annual mailing to individuals then covered by the Plan.
  - b. **Three Years.** The Plan must notify individuals covered by the Plan, at least once every three years, of the availability of the Privacy Notice and how they can obtain a copy of the Privacy Notice.
2. **Availability of Privacy Notice**
  - a. **Electronic Notice.** (45 C.F.R. §164.520(c)(3)).
    - (i) The Plan will prominently post its Privacy Notice on its website, and make the Privacy Notice available electronically through said website at [levycounty.org](http://levycounty.org). The Plan may provide the Privacy Notice to an individual by e-mail if the individual agrees to receive the Privacy Notice in such manner. If the Plan becomes aware that e-mail transmission has failed, a paper copy of the Privacy Notice will be provided to the individual. Additionally, an individual receiving a copy of the Privacy Notice by e-mail always maintains the right to obtain a paper copy of Privacy Notice from the Plan upon request.
  - b. **Paper Copy of Notice.** Individuals have a right to a paper copy of the Privacy Notice, even if they have previously agreed to receive the Privacy Notice electronically. Individuals may receive a copy of the Privacy Notice by:

- (i) In-person request to the Privacy Officer;
- (ii) Written Request. An individual can submit a request for Privacy Notice in writing to:

**Human Resource Manager  
Levy County Commission  
PO Box 310, Bronson, FL 32621  
352-486-5219 phone  
martin-jacqueline@levycounty.org**

- C. **DOCUMENTATION.** The Plan will retain copies of the Privacy Notices issued by it for six (6) years in accordance with 45 C.F.R. §164.530(j) and Policy XX. (45 C.F.R. §164.520(e))

**XIX. POLICY SUBJECT: ENFORCEMENT; SANCTIONS FOR NON-COMPLIANCE**

**POLICY:** The Plan will apply appropriate sanctions against its Plan Sponsor Employees, Authorized Employees and Business Associates who fail to comply with these privacy policies and procedures or the requirements of the Privacy Rule. (45 C.F.R. §164.530(e)(1))

**A. SANCTIONS FOR NON-COMPLIANCE**

Any Plan Sponsor Employees who violate the Privacy Rule and/or these policies and procedures will be subject to sanctions, which may include verbal counseling, write-ups, suspension and/or termination.

**B. EXEMPTIONS.**

1. **Whistleblower.** No violation may be considered to have been committed if a Plan Sponsor Employee (45 C.F.R. §164.502(j)(1)(ii)):
  - a. Discloses PHI with a good faith belief that the Plan has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the Plan potentially endangers one or more patients, workers, or the public and the disclosure is to:
    - (i) A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the Plan or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the Plan; or,
    - (ii) An attorney retained by or on behalf of the workforce member or Business Associate for the purpose of determining legal options with regard to whether the Plan has engaged in conduct that is unlawful or otherwise violates professional or clinical standards or that the care, services, or conditions provided by the Plan potentially endangers one or more patients, workers, or the public.
2. **Victims of a Crime.** No violation can be considered to have been committed where a Plan Sponsor Employee, who is the victim of a criminal act, discloses PHI to a law enforcement official, provided that (45 C.F.R. §164.502(j)(2)):

- a. The PHI disclosed is about the suspected perpetrator of the criminal act; and
  - b. The PHI is limited to the information listed in 45 C.F.R. §164.512(f)(2)(i).
- C. **DOCUMENTATION.** All sanctions that are applied will be documented and any related records will be retained for six (6) years in accordance with 45 C.F.R. §164.530(j) and Policy XX.

XX. **POLICY SUBJECT: DOCUMENTATION AND RECORDS RETENTION**

**POLICY:** The Plan will maintain a written or electronic record of certain documentation, in accordance with this policy. (45 C.F.R. §164.530(j))

**DOCUMENTATION.** The following documents must be maintained: HIPAA divides the documents that need to be retained into the following three categories:

- A. **Policies and Procedures:** The Plan must document any changes in its privacy practices in its policies and procedures, and maintain the revised policies and procedures in accordance with the document retention requirements.
1. The Privacy Officer is responsible for making the changes.
  2. The Privacy Officer is responsible for maintaining documentation of all changes.
  3. The Privacy Officer must ensure the latest version of the Policies and Procedures Document is on site.
- B. **Written Documentation Required to be Retained by the Plan:** The Privacy Officer is required to retain any action, activity or designation action, which is required to be in writing, be kept in the HIPAA file or an electronic copy. The written communications and actions, activities or designations required to be documented are:
1. Personnel Designations;
  2. Training materials, dates of training, logs with participant names and signatures;
  3. Authorizations obtained by the Plan (Individual/Family);
  4. Complaints and subsequent actions;
  5. Notice of Privacy Rights and subsequent revisions;
  6. Individual Rights Requests, Responses/Denials;
    - a. Rights to Restrict Privacy Protection for Protected Health Information;
    - b. Rights to Request Confidential Communications by Alternative Means or at Alternative Location;
    - c. Individual's Access to Protected Health Information: the designated record sets that are subject to access by individuals as provided by the designated Business Associates;
    - d. Amended Health Information;
    - e. Accounting of Disclosures.

7. PHI as outlined in Policy III.A of this document;
8. Any disclosures or uses of PHI that could potentially constitute a breach, the results of the investigation into whether a breach has occurred, and any notifications sent due to the breach.
9. Any of the above referenced documentation as provided by an Authorized Business Associate.

C. **RECORDS RETENTION.** The Plan will retain the above-described required documentation for six years from the date of its creation or the date when it was last in effect, whichever is later. (45 C.F.R. §164.530(j)(2)).

**ADDENDUM A**

**PUBLIC RISK MANAGEMENT OF FLORIDA (“THE PLAN”)**

**AUTHORIZED EMPLOYEES**

The following is a listing of the employees who the Plan Sponsor has granted limited access of PHI who need such access to carry out their duties.

Authorized Employee Name	Authorized Employee Title
Jacqueline Martin, Levy County Commission	Human Resource Manager
Karen Blackburn, Levy County Commission	Human Resource Assistant
Ann Moody, Clerk's Office	Deputy Clerk – Finance
Sandy Haddock, Clerk's Office	Deputy Clerk – Human Resource
Tammy Jones, Supervisor of Elections	Elected Official
Linda Fugate, Tax Collector	Elected Official
Michelle, Heddins, Tax Collector’s Office	Finance Director
Osborn Barker, Property Appraiser	Elected Official
Lisa Shipp, Property Appraiser’s Office	Administrative Assistant

**ADDENDUM B**

**PUBLIC RISK MANAGEMENT OF FLORIDA (“THE PLAN”)**

**FAMILY AUTHORIZATION TO DISCLOSE  
PROTECTED HEALTH INFORMATION**

The Health Insurance Portability and Accountability Act (“HIPAA”) privacy regulations become effective on **April 14, 2003**. The privacy regulations generally require, among other things, that the Plan only disclose Protected Health Information (“PHI”) to the individual who is the subject of that information or pursuant to an authorization from that individual. For example, except in certain circumstances, the Plan may not disclose a participant’s PHI to a spouse, or an adult dependent’s PHI to the participant or spouse, or the spouse’s PHI to the participant. (Generally, a minor child’s PHI may be disclosed to either parent or legal guardian without an authorization.) Any adult individual, however, may authorize family members or others to have that individual’s PHI disclosed to them. You and/or any of your adult dependents may do so by each completing the following authorization. Or, you and/or each of your adult dependents may complete an authorization each time that you or they want specific health information disclosed to a family member or another person. You can also choose not to authorize the Plan to share your health information with any family members or other persons.

\*\*\*\*\*

1. My name is \_\_\_\_\_, my date of birth is \_\_\_\_\_ (If I am a dependent, the participant through whom I am insured is \_\_\_\_\_ and his/her date of birth is \_\_\_\_\_).

I hereby authorize my health information to be disclosed as described in this Authorization.

2. I hereby request and authorize the Plan to release health information about me to my family members or others identified in Section 5 that relates to the following: my health claims and eligibility records, including oral and written information such as, but not limited to, claims detail, claims status, payment records, Explanation of Benefits forms, and Coordination of Benefits.
3. This health information is to be used by my family members or others identified in Section 5 for the purposes of assisting me in obtaining necessary medical care, filing health care claims on my behalf, checking on the status of health care claims that have been filed on my behalf, and working with the Plan to work out any other issues that may arise with respect to the health benefits that are provided to me by the Plan.

4. I also request that the following limitations be placed on the disclosure of my health information to my family members or others identified in Section 5: *(This section should only be filled out if you wish to limit the disclosures of your health information to your family members or others identified in Section 5.):*

---

---

---

5. I authorize my above-described health information to be disclosed only to the following identified individuals. *(There is no limit to the number of individuals you can list in this section.)*

Name and date of birth	Describe Relationship <i>(i.e., husband, wife, parent, friend, other)</i>
------------------------	---

Name and date of birth	Describe Relationship <i>(i.e., husband, wife, parent, friend, other)</i>
------------------------	---

Name and date of birth	Describe Relationship <i>(i.e., husband, wife, parent, friend, other)</i>
------------------------	---

Name and date of birth	Describe Relationship <i>(i.e., husband, wife, parent, friend, other)</i>
------------------------	---

6. I understand that the Plan may not condition my treatment, payment, enrollment, or eligibility for benefits on whether I agree to sign this Authorization.

7. I understand that once my health information is disclosed pursuant to this Authorization, the federal privacy protections may no longer apply to the disclosed health information, and thus, my family member(s) and others described in Section 5 to whom my health information is disclosed may re-disclose that health information.

8. I understand that I am entitled to receive a copy of this authorization.

9. I understand that I have the right to revoke this Authorization at any time by sending a letter to the Plan's Privacy Officer, \_\_\_\_\_ (insert name/title, and contact information of HIPAA Privacy Officer). The revocation will take effect on the date that it is received by the Privacy Officer, as applicable. I further understand that any revocation will be effective only to the extent that the Plan has not already disclosed my health information based on this Authorization.
10. This Authorization will expire at the end of my enrollment in the Plan (*or some other expiration date or event*).

\_\_\_\_\_  
Print Name

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

**ADDENDUM C**

**AUTHORIZATION FOR THE  
PUBLIC RISK MANAGEMENT OF FLORIDA (“THE PLAN”)  
TO USE OR DISCLOSE PROTECTED HEALTH INFORMATION**

My name is \_\_\_\_\_, and my date of birth is: \_\_\_\_\_. (If I am a dependent, the participant through whom I am insured is \_\_\_\_\_ and his/her date of birth is \_\_\_\_\_). I hereby authorize the Plan to disclose protected health information (“PHI”) about me as described below:

1. The information to be disclosed is \_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_

*[Describe health information to be disclosed in a specific and meaningful fashion]*

2. \_\_\_\_\_ *[name and/or title of employee or department authorized to make the disclosure]* may disclose the above-described information to \_\_\_\_\_ *[name of person(s) or organization to whom the health information may be disclosed]*.

3. This disclosure is made for the following purposes: \_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_

*[Each purpose for the requested disclosure must be described. If the individual initiates the authorization, the statement “at the request of the individual” is a sufficient description of the purpose.]*

4. I understand that the Plan is not conditioning my treatment, payment, enrollment, or eligibility for benefits on whether I agree to sign this authorization.

5. I understand that the information disclosed pursuant to this authorization may no longer be protected by the federal health privacy rule and may be subject to re-disclosure by the recipient.

6. I understand that I have the right to revoke this authorization in writing at any time by sending a letter to the Plan's Privacy Officer, Jacqueline Martin, Human Resource Manager, phone 352-486-5219, email: martin-jacqueline@levycounty.org and that the effective date of my revocation will be the date of receipt by the Privacy Officer. I further understand that any revocation will be effective only to the extent that the Plan has not already taken action in reliance on this authorization.
7. I understand that I am entitled to receive a copy of this authorization.

This Authorization shall expire on the date of termination of my enrollment in the Plan.  
*(other expiration date or event may be indicated).*

\_\_\_\_\_  
 Printed Name (of person giving authorization)

\_\_\_\_\_  
 Signature of person giving authorization

\_\_\_\_\_  
 Date

\_\_\_\_\_  
 Name of personal representative (if applicable)

\_\_\_\_\_  
 Relationship to person giving authorization

\_\_\_\_\_  
 Date

\_\_\_\_\_  
 Description of representative's authority to act for the individual

**ADDENDUM D**

**AUTHORIZATION TO HEALTHCARE PROVIDERS TO DISCLOSE  
PROTECTED HEALTH INFORMATION TO THE COMPANY**

Explanation of this Form: The Health Insurance Portability and Accountability Act (“HIPAA”) privacy regulations become effective on **April 14, 2003**. The privacy regulations generally require, among other things, that health care providers disclose Protected Health Information (“PHI”) to the individual who is the subject of that information or pursuant to an authorization from that individual. PHI is defined by HIPAA, but generally includes any personal health information. The purpose of this Authorization is to authorize the health care provider(s) who perform your pre-employment physical or employment drug test to release the results of that physical or test to \_\_\_\_\_ (“Company”).

\*\*\*\*\*

1. My name is \_\_\_\_\_, I hereby authorize my PHI to be disclosed as described in this Authorization.
  
2. The information to be disclosed is (circle as applicable):
  - a. The results of my employment drug test on \_\_\_\_\_ (date).
  - b. The results of my pre-employment physical on \_\_\_\_\_ (date).
  
2. \_\_\_\_\_ **[Name of Health Care Provider]** may disclose the above described information to the **Human Resources/Risk Management Department** at the Company.
  
3. This disclosure is made for the purpose of determining my fitness for duty as an employee of the Company.
  
4. I understand that the provision of the employment drug test or pre-employment physical is conditioned on my signing this Authorization.
  
5. I understand that once my PHI is disclosed pursuant to this Authorization, the federal privacy protection will no longer apply to the disclosed PHI, and thus, the recipient of my PHI may re-disclose it. However, it is my understanding that the Company will protect my PHI that it receives pursuant to this Authorization in accordance with other, applicable federal and state laws.
  
7. I understand that I have the right to revoke this Authorization at any time by sending a written notice to \_\_\_\_\_ **[Name of Health Care Provider]** at:  
\_\_\_\_\_.
  
8. I understand that the revocation will take effect on the date that it is received by  
\_\_\_\_\_.

**[Name of Health Care Provider].**

However, I understand that any revocation will be effective only to the extent that

---

**[Name of Health Care Provider].**

has not already disclosed my health information based on this Authorization.

9. This Authorization will expire at the time that my fitness for duty is determined by the Company.

---

Printed Name of person giving authorization

---

Signature of person giving authorization

---

Date

**[The individual must be furnished with a signed copy.]**

## **ADDENDUM E – NOTICE OF PRIVACY PRACTICES**

### **PUBLIC RISK MANAGEMENT OF FLORIDA** **(“THE PLAN”)**

#### **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.**

**This Notice applies to the Plan’s self-insured health benefit options. If you participate in the insured dental plan or vision services benefit options, you may also receive a separate notice directly from the insurer.**

#### **THE PLAN’S COMMITMENT TO PRIVACY**

The Plan is committed to protecting the privacy of your protected health information (“health information”). Health information is information that identifies you and relates to a physical or mental condition, or to the provision or payment of health services for you. The Plan also pledges to provide you with certain rights related to your health information.

By this Notice of Plan’s Privacy Practices (“Notice”), the Plan informs you that it has the following legal obligations under the federal health privacy provisions contained in the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) and the related regulations (“federal health privacy law”):

- To maintain the privacy of your health information;
- To provide you with this Notice of its legal duties and privacy practices with respect to your health information; and
- To abide by the terms of this Notice currently in effect.

This Notice also informs you how the Plan uses and discloses your health information and explains the rights that you have with regard to your health information maintained by the Plan. For purposes of this Notice, “you” and “yours” refers to participants and dependents that are eligible for benefits described under the Plan.

This Notice is effective as of **September 23, 2013**, and will remain in effect unless and until the Plan issues a revised Notice. This supersedes any Notice of Privacy Practices issued prior.

#### **INFORMATION SUBJECT TO THIS NOTICE**

Only health information that may specifically identify you *and* is collected or maintained by the Plan *and* relates to the health benefits offered under the Plan is protected under HIPAA. Health benefits include: Medical, dental, healthcare flexible spending accounts, vision benefits and employee assistance programs.

#### ***This Notice does not apply to the following information:***

Health information collected or maintained by your employer and/or the Plan that relates to non-health employee benefits, including disability benefits, life insurance, accidental death and dismemberment insurance, pre-paid legal services, business travel and accident insurance, and workers’ compensation insurance.

Health information that your employer requests, receives, and maintains about you for employment purposes, such as for example, employment testing, or determining your eligibility for medical leave benefits under the Family and Medical Leave Act or retirement benefits or disability accommodations under the Americans With Disabilities Act.

Third parties assist the Plan in administering your health benefits (such as Florida Blue, Gallagher Benefit Services, Inc., Businessolver, Inc. and others). They are referred to as Business Associates. These Business Associates generate, maintain, use, and disclose most of the health information maintained by the Plan about the healthcare services you receive and the payments for such services. They use this information to process your benefit claims and are required to use the same privacy protections as the Plan. In addition, your healthcare providers (such as doctors and hospitals) also maintain some of your information. You should ask your healthcare providers directly if you have any questions about health information maintained by them.

## SUMMARY OF THE PLAN'S PRIVACY PRACTICES

### *The Plan's Uses and Disclosures of Your Health Information*

Generally, you must give your written authorization to the Plan in order for the Plan to use and/or disclose your health information. However, the Plan may use and disclose your health information without your authorization for the administration of the Plan and for processing claims. The Plan also may use and disclose your health information without your authorization for other purposes as permitted by the federal health privacy law, such as health and safety, law enforcement or emergency purposes. The details of the Plan's uses and disclosures of your health information are described below.

### *Your Rights Related to Your Health Information*

The federal health privacy law provides you with access to your health information and with certain rights related to your health information. Specifically, you have the right to:

- Inspect and/or copy your health information;
- Request to receive your health information through confidential communications;
- Request that your health information be amended;
- Request an accounting of certain disclosures of your health information;
- Request certain restrictions related to the use and disclosure of your health information;
- File a complaint with the Plan or the Secretary of the Department of Health and Human Services if you believe that your privacy rights have been violated; and
- Receive a paper copy of this Notice.

These rights and how you may exercise them are detailed below.

### *Changes in the Plan's Privacy Policies*

The Plan reserves its right to change its privacy practices and revise this Notice as described below.

### *Contact Information*

If you have any questions or concerns about the Plan's privacy practices, or about this Notice, or you wish to obtain additional information about the Plan's privacy practices, please contact:

#### **Privacy Officer:**

**Human Resource Manager  
Levy County Commission  
PO Box 310, Bronson, FL 32621  
352-486-5219 phone  
martin-jacqueline@levycounty.org**

## DETAILED NOTICE OF THE PLAN'S PRIVACY PRACTICES

### THE PLAN'S USES AND DISCLOSURES

The Plan only uses and discloses your health information as described in this Notice. The uses and disclosures that do not require your written authorization are described below.

#### *Uses and Disclosures for Treatment, Payment, and Health Care Operations*

1. **For Treatment.** The Plan may use and disclose your health information, without your authorization, to a health care provider, such as a hospital or physician, to assist the provider in treating you. For example, the Plan may disclose to a treating orthodontist the name of your treating dentist so that the orthodontist may ask for your dental X-rays.
2. **For Payment.** The Plan may use and disclose your health information, without your authorization, so that your claims for health care treatment, services and supplies can be paid according to the Plan's terms. For example, the

Plan may tell a doctor whether you are eligible for coverage or what percentage of the bill will be paid by the Plan.

3. **For Health Care Operations.** The Plan may use or disclose your health information, without your authorization, to enable it to operate efficiently and in the best interests of its participants. For example, the Plan may use information about your claims to project future benefit costs or audit the accuracy of its claims processing. However, the Plan may not use or disclose any health information that is genetic information for purposes of underwriting.

#### ***Uses and Disclosures to Business Associates***

The Plan discloses your health information, without your authorization, to its Business Associates, which, as explained above, are third parties that assist the Plan in its operations. For example, the Plan may share your health information with a Business Associate that processes health care claims for the Plan, or for the purpose of enabling the Business Associate to provide you with assistance with resolution of a claim. The Plan enters into agreements with its Business Associates to ensure that the privacy of your health information is protected from unauthorized disclosure.

#### ***Uses and Disclosures to the Plan Sponsor***

The Plan may disclose health and eligibility information, without your authorization, to certain benefits personnel of the Plan Sponsor, such as verifying claims payment information, for quality assurance functions, or for auditing and monitoring purposes. The Plan Sponsor does not typically have access to diagnosis or any other specific details about claims. Your health information cannot be used for employment purposes, however, without your specific authorization.

#### ***Other Uses and Disclosures That May Be Made Without Your Authorization***

The federal health privacy law provides for specific uses or disclosures of your health information that the Plan may make without your authorization, which are described below.

1. **Required by Law.** The Plan may use and disclose health information about you as required by federal, state or local law.
2. **Additional Legal Reasons.** The Plan may disclose your health information for the following purposes:
  - a. For judicial and administrative proceedings pursuant to court or administrative order, subpoena or other legal process.
  - b. To report information related to victims of abuse, neglect, or domestic violence.
  - c. To law enforcement officials for certain law enforcement duties.
3. **Health and Safety.** Your health information may be disclosed to avert a threat to the health or safety of you, any other person, or the public, consistent with applicable law. Your health information also may be disclosed for public health activities, such as preventing or controlling disease, injury or disability.
4. **Government Functions.** Your health information may be disclosed to the government for specialized government functions, such as intelligence, national security activities, and protection of public officials. Your health information also may be disclosed to health oversight agencies that monitor the health care system for audits, investigation, licensure, and other oversight activities.
5. **Active Members of the Military and Veterans.** Your health information may be used or disclosed to comply with laws and regulations related to military service or veterans' affairs.
6. **Workers' Compensation.** Your health information may be used or disclosed in order to comply with laws related to Workers' Compensation.
7. **Emergency Situations.** Your health information may be used or disclosed to a family member or close personal friend involved in your care in the event of an emergency, or to a disaster relief entity in the event of a disaster.
8. **Others Involved In Your Care.** In limited instances, your health information may be used or disclosed to a family member, close personal friend, or others who the Plan has verified are involved in your care or payment for your care. For example, if you are seriously injured and unable to discuss your case with the Plan, the Plan may so disclose your health information. Also, in certain instances, the Plan may advise a family member or close personal friend about your general condition, location (such as in the hospital) or death. If you do not want this information to be shared, you may request that these disclosures be restricted as outlined later in this Notice.
9. **Personal Representatives.** Your health information may be disclosed to people you have authorized or people who have the right to act on your behalf. Examples of personal representatives are parents for minors, and those who have Power of Attorney for adults.
10. **Treatment and Health-Related Benefits Information.** The Plan and its Business Associates may contact you to provide information about treatment alternatives or other health-related benefits and services that may interest you, including, for example, alternative treatment, services or medication.

11. **Research.** Under certain circumstances, the Plan may use or disclose your health information for research purposes, as long as the procedures required by law to protect the privacy of the research data are followed.
12. **Organ and Tissue Donation.** If you are involved with an organ donation, your health information may be used or disclosed to an organ donor, eye, or procurement organization to facilitate an organ or tissue donation or transplantation.
13. **Deceased Individuals.** The health information of a deceased individual may be disclosed to coroners, medical examiners, and funeral directors so that those professionals can perform their duties.

#### ***Uses and Disclosures for Fundraising and Marketing Purposes***

The Plan does not use your health information for fundraising or marketing purposes.

#### ***Any Other Uses and Disclosures Require Your Express Authorization***

Uses and disclosures of your health information *other than* those described above will be made only with your express written authorization. You may revoke your authorization in writing. If you do so, the Plan will not use or disclose your health information authorized by the revoked authorization, except to the extent that the Plan already has relied on your authorization.

Once your health information has been disclosed pursuant to your authorization, the federal privacy protections may no longer apply to the disclosed health information, and that information may be re-disclosed by the recipient without your or the Plan's knowledge or authorization.

#### ***Minimum Necessary Standard***

The Plan will make reasonable efforts not to use, disclose or request more than the minimum amount of health information necessary to accomplish the intended purpose of the use, disclosure, or request. The "minimum necessary" standard will not apply, however, to certain disclosures, such as disclosures of your health information to you.

## **YOUR HEALTH INFORMATION RIGHTS**

You have the following rights regarding your health information that the Plan collects and maintains. If you are required to submit a written request related to these rights, as described below, you should address such requests to the Privacy Officer noted above.

#### ***Right to Inspect and Copy Health Information***

You have the right to inspect and obtain a copy of your health information. This includes, among other things, health information about your Plan eligibility; Plan coverages, claim records, and billing records. For health information for which you have a right of access, you have the right to receive your health information in an electronic format if it is readily producible in such format, and to direct the Plan to transmit a copy of your health information to an entity or person you designate, provided the designation is clear, conspicuous and specific.

To inspect and copy your health information maintained by the Plan, submit your request in writing to the Privacy Officer. The Plan may charge a fee for the cost of copying your health record, and may charge you the cost of mailing your health record to you. In certain limited circumstances, the Plan may deny your request to inspect and copy your health record. If the Plan does so, it will inform you in writing. In certain instances, if you are denied access to your health record, you may request a review of the denial.

#### ***Right to Request Confidential Communications, or Communications by Alternative Means or at an Alternative Location***

You have the right to request that the Plan communicate your health information to you in confidence by alternative means or in an alternative location. For example, you can ask that the Plan only contact you at work or by mail, or that the Plan provide you with access to your health information at a specific location.

To request confidential communications by alternative means or at an alternative location, submit your request in writing to the Privacy Officer. Your written request should state the reason(s) for your request and the alternative means by or location at which you would like to receive your health information. If appropriate, your request should state that the disclosure of all or part of your health information by non-confidential communications could endanger you. The Plan will accommodate reasonable requests and will notify you appropriately.

### ***Right to Request That Your Health Information Be Amended***

You have the right to request that the Plan amend your health information if you believe the information is incorrect or incomplete.

To request an amendment, submit a detailed request in writing to the Privacy Officer, providing the reason(s) that support your request. The Plan may deny your request if you have asked to amend information that:

- Was not created by the Plan, unless you provide the Plan with information that the person or entity that created the information is no longer available to make the amendment;
- Is not part of your health information maintained by or for the Plan;
- Is not part of the information which you would be permitted to inspect and copy; or
- Is accurate and complete.

The Plan will notify you in writing as to whether it accepts or denies your request for an amendment to your health information. If the Plan denies your request, it will explain the reason(s) for the denial, and describe how you can continue to pursue the denied amendment.

### ***Right to an Accounting of Disclosures***

You have the right to receive a written accounting of disclosures. The accounting is a list of disclosures of your health information by the Plan to others, except that disclosures for treatment, payment or health care operations, disclosures made to or authorized by you, and certain other disclosures are not part of the accounting. The accounting covers up to six years prior to the date of your request, except that the accounting will not include disclosures the Plan made before April 14, 2003. If you want an accounting that covers a time period of less than six years, please state that in your written request for an accounting.

To request an accounting of disclosures, submit your request in writing to the Privacy Officer. Your request should indicate in what form you want the accounting (for example, paper or electronic). The first accounting that you request within a twelve-month period will be free. For additional accountings in a twelve-month period, the Plan will charge you for the cost of providing the accounting, but the Plan will notify you of the cost involved before processing the accounting so that you can decide whether to withdraw your request before any costs are incurred.

### ***Right to Request Restrictions***

You have the right to request restrictions on your health care information that the Plan uses or discloses about you to carry out treatment, payment or health care operations. Also, you have the right to request restrictions on your health information that the Plan discloses to someone who is involved in your care or the payment for your care, such as a family member or friend. The Plan is not required to agree to your request for such restrictions, and the Plan may terminate its agreement to the restrictions you requested.

To request restrictions, submit your request in writing to the Privacy Officer stating what information you seek to limit, and how and/or to whom you would like the limit(s) to apply. The Plan will notify you in writing as to whether it agrees to your request for restrictions. The Plan will also notify you in writing if it terminates an agreement to the restrictions that you requested.

### ***Right to Receive Notification of a Breach of Unsecured Health Information***

You have the right to receive notice if your unsecured health information is disclosed in violation of HIPAA unless there is a low probability that the health information has been compromised. If it is determined from the Plan's risk assessment that a breach has occurred, you will be notified without unreasonable delay and no later than 60 days after discovery of the breach. The notification will include information about what happened and what may be done to mitigate any harm.

### ***Right to Complain***

You have the right to complain to the Plan and/or to the U.S. Department of Health and Human Services, Office for Civil Rights if you have concerns about the Plan's privacy policies and procedures (including its breach notification policies and procedures) or about the Plan's use or disclosure of your health information.

To file a complaint with the Plan, submit a detailed written description of the problem to the Privacy Officer. To file a complaint with the U.S. Department of Health and Human Services, submit a detailed written description of the problem to your regional Office for Civil Rights. Your description must name the covered entity (the Plan) and what action (or lack of action) you believe has violated HIPAA. Your complaint must be submitted within 180 days of when you knew or should have known of the problem, unless this deadline is waived by the Office for Civil Rights. For contact information and to find your regional Office for Civil Rights, see the Privacy Officer.

You will not be retaliated or discriminated against and no services, payment, or privileges will be withheld from you because you file a complaint with the Plan or with the U.S. Department of Health and Human Services, Office for Civil Rights.

If you have any questions concerning how to file a complaint, please contact the Privacy Officer.

***Right to a Paper Copy of This Notice***

You have the right to a paper copy of this Notice. To make such a request, submit a written request to the Privacy Officer.

***For more information***

***For information regarding the U.S. Department of Health and Human Services and to find the address for your regional Office for Civil Rights, log on to:***

<http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html>

***You may also submit any request to the Privacy Officer who will forward your request to the appropriate Plan privacy contact.***

---

**CHANGES IN THE PLAN'S PRIVACY PRACTICES**

The Plan reserves the right to change its privacy practices and make the new practices effective for all health information that it maintains, including your health information that it created or received prior to the effective date of the change and your health information it may receive in the future. If the Plan materially changes any of its privacy practices covered by this Notice, it will revise its Notice and distribute the revised version of the Notice or information about the material change to affected individuals in the next annual mailing to participants.