INTERNAL PRIVACY POLICIES AND PROCEDURES

ALLEGIANCE BENEFIT PLAN MANAGEMENT, INC.

For more information,
Contact Allegiance's Privacy Official

TABLE OF CONTENTS

OVERVIEW OF HIPAA PRIVACY REGULATIONS AND REQUIREMENTS

Federal privacy regulations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) require group health plans to comply with certain rules for sharing and disclosing an individual's Protected Health Information (PHI). HIPAA provides individuals with the right to access their PHI, the right to amend or append their PHI and the right to request restrictions on use and disclosure of their PHI. Compliance with the HIPAA privacy regulation was required by April 14, 2003.

Allegiance Benefit Plan Management, Inc. (Allegiance) may provide PHI to treating health care providers and insurers as necessary for payment and health care operations and to plan administrators as necessary for plan administration functions.

> **Health care operations** are activities such as quality assessment or improvement activities, outcomes measurement, population-based activities related to improving health or reducing costs, protocol development, preventive health activities, case management or care coordination, contacting providers or patients with alternative treatment options, reviewing qualifications of healthcare providers and evaluating their performance, evaluating health plan performance, conducting training of healthcare professionals, accreditation, certification, licensing or credentialing activities, auditing functions, underwriting and premium rating activities, plan funding activities, including obtaining stop-loss coverage and forecasting plan liability on high-dollar claims, compliance programs, cost-management activities, responding to appeals, external reviews, or internal grievances, arranging for medical reviews and auditing, and customer service activities.
>
> **Payment activities** include obtaining premiums, determining eligibility or coverage limits and reimbursing providers. Examples of payment activities include coordination of benefits, adjudication and subrogation of claims, risk adjusting amounts based upon enrollee health status and demographics, billing, claims management, obtaining payment under a contract for reinsurance, related data processing, reviews of claims related to medical necessity or appropriateness of care, and utilization review activities.
>
> **Plan administration functions** include most of the activities listed under health care operations or payment activities.

Although Allegiance is not a covered entity with respect to the third party administrative services it provides, Allegiance receives PHI. Allegiance must therefore use and disclose this PHI in the same manner as the covered entities (group health plans) that Allegiance provides services to. To determine eligibility, adjudicate claims, and pay benefits for these group health plans, Allegiance must comply with those HIPAA privacy rules as a business associate of its client group health plans.

Definition of Protected Health Information (PHI)

PHI is individually identifiable health information or health information that reasonably identifies an individual, including the individual's demographic information, that:

(a) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

(b) Relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for health care received by an individual.

(c) Is transmitted or maintained in any form, paper or electronic. Electronic transmission includes the Internet, network connections between Allegiance and other corporate networks, leased lines, dial-up lines, private networks, and any transmissions using magnetic tape, disk or CD-Rom.

PHI does not include employment records held by the Plan sponsor (employer) in its role as an employer. These employment records may include: medical information used by the employer to carry out its obligations under the Family Medical Leave Act, American Disabilities Act, and other similar laws, and records related to occupational injuries, disability insurance eligibility, sick leave requests and justifications, drug screening requests, workplace medical surveillance, and fitness for duty requests.

Who is Subject to HIPAA?

HIPAA applies to Allegiance's client group health plans, Allegiance's own employee group health plan, Allegiance Life & Health and any health care clearinghouses and health care providers with which Allegiance interacts.

This Privacy Manual explains how Allegiance may use and/or disclose PHI it receives, how an individual may access or amend any PHI that Allegiance receives, and what administrative procedures Allegiance must implement and maintain to protect the privacy of PHI it receives.

Allegiance's Privacy Procedure Requirements

I. Appoint a Privacy Official

a. The Privacy Official is responsible for the development of an internal privacy policy, an employee training program, and ongoing monitoring of Allegiance's business practices and activities to ensure that PHI is properly safeguarded and used or disclosed in a manner compliant with HIPAA. The Privacy Official may select staff to participate on an internal Privacy Team to foster interdepartmental communication and coordinate compliance activities.

b. The Privacy Official is Alan Hall, V.P., General Counsel, extension 3100.

II. Development of Policies and Procedures

a. Allegiance will develop internal privacy policies and administrative practices to ensure PHI is protected and that access to, use of and disclosure of PHI is restricted consistent with HIPAA and the HITECH Act. The policies explain how Allegiance collects information, what type of information Allegiance may collect, how Allegiance may use PHI it receives, and how Allegiance may disclose PHI to others. **All PHI must be handled in accordance with this Privacy Manual.**

b. Allegiance will change its privacy policies and procedures as necessary and appropriate to comply with changes in the law.

c. If changes to Allegiance's privacy policies and procedures affects benefit management services to clients, Allegiance will notify clients of any changes.

d. If changes to privacy policies and procedures affect the content of Allegiance's Notice of Privacy Practices (Notice), Allegiance will promptly revise the Notice. Allegiance must abide by the terms of the Notice currently in effect until a revised notice has been provided. See Appendix A for a copy of Notice.

e. Allegiance will document all changes to its privacy policies and procedures and the effective date of such changes and retain this documentation for at least six years.

III. Training for Members of Allegiance' workforce

a. Allegiance will train all members of its workforce on its privacy policies and procedures within a reasonable period of time after the person joins Allegiance's workforce.

b. Allegiance will train all members of its workforce on material changes to its privacy policies and procedures within a reasonable time of the effective date of the changes.

c. Allegiance will document all training received by its workforce.

d. Allegiance will have appropriate sanctions for those members of its workforce who use or disclose PHI in violation of its privacy practices and procedures.

IV. Safeguards for PHI

a. Allegiance will reasonably safeguard PHI from intentional or unintentional uses or disclosures in violation of HIPAA, and the HITECH Act through the use of appropriate administrative, technical and/or physical measures.

- **i.** Procedural safeguards can include providing only the minimum necessary PHI, limiting access to PHI to individuals with a legitimate need to know, limiting access to claims information and recording all telephone conversations concerning claims and benefits.
- **ii.** Electronic safeguards can include electronic claims submission, secured storage and retrieval of electronic information and use of computer passwords to access PHI.
- **iii.** Physical safeguards can include storing original documents in a secure storage area, subsequently shredding or returning to the client group health plan at the end of the agreed upon retention period, and placing discarded materials in a secured location until shredded or recycled.

b. Allegiance will mitigate as much as reasonably practicable, any harm it knows of from inappropriate uses or disclosures of PHI.

c. The privacy official will conduct voluntary internal audits pursuant to the Audit Protocol for Health Information Privacy as promulgated by the US Department of Health & Human Services in conjunction with the company's security official. This audit shall be conducted annually.

V. Process for Complaints

a. Allegiance will develop and implement a process through which individuals may make complaints about Allegiance's

privacy policies and procedures. Allegiance's Notice will outline this process.

b. Complaints received and the resolution of each complaint will be documented, if any.

c. Allegiance will not intimidate, threaten, coerce, discriminate against or take any other retaliatory action against an individual who makes a complaint.

VI. Requirements Related to Client Group Health Plans

a. Allegiance will have Business Associate Agreements with client group health plans to protect the confidentiality of PHI it uses or discloses for or on the behalf of its client group health plans.

b. If the client's relationship with Allegiance ends, Allegiance will continue to protect the privacy of PHI according to its privacy policies then in effect and applicable law.

c. If an individual's coverage through a client group health plan ends, Allegiance will continue to protect the privacy of that individual's PHI according to its privacy policies then in effect and applicable law.

d. Summary Plan Documents will be amended as necessary, to ensure that Plan Administrator/Plan Sponsor (employers) protect the confidentiality of PHI they receive for plan administration.

e. Notice of Privacy Practices for client group health plans to be developed and updated as necessary. Notice to be available on the abpmtpa.com website and in paper copy, upon request to the Plan Administrator. Notice may be e-mailed to any participant if the participant agrees

i. Notice (or availability of the Notice) to be distributed as follows:

1. To any participant upon enrollment with his or her group health plan;

2. To all covered participants within 60 days of material changes to the Notice;

3. To all covered participants every three years of the availability of the Notice (if no material changes).

VII. Breach or Attempted Breach Handling

Allegiance through its I.T. Department will determine whether or not a system has been compromised. If there is positive evidence of a compromise, IT shall immediately do the following:

- Isolate the compromised system from the rest of the network.
- Determine the mechanism by which the attack is performed and take appropriate action. For something like an e-mail virus, for example, it should be sufficient to remove only the computers that have received the email from the network. For something more serious, like a virus that spreads to other computers on the local network, or an unauthorized remote login, it must be assumed that all computers on the attached network segment and connected networks with lower security are compromised. (If an internal machine has been compromised, it must be assumed that all internal systems have been compromised, as well as those on the DMZ.)
- Remove remaining compromised systems from the network.
- Attempt to determine the origin of the breach Notify the appropriate authorities.
- Reinstall each compromised system, from scratch, making sure to reformat all file systems as part of the install.
- Program files must not be restored from backup; they must be reinstalled from installation media. Locally developed programs must be recompiled from source, and then reinstalled in the appropriate locations.
- Compromised systems must not be reconnected to the main network until they've been reinstalled.
- Assume any data on compromised systems has been leaked. All passwords must be changed; keys and certificates must be re-issued.
- Compromised web servers with SSL capability must get new certificates from the certificate authority.
- If a compromised system contains PHI, affected parties must be notified. The notice will contain a brief description of the security breach, a description of the types of information involved in the breach (name, SSN, etc.), any steps the individual should take to protect themselves from harm resulting from the breach, a brief description of the steps we're taking to mitigate harm to them and prevent further breaches, and contact

procedures for individuals to ask questions and learn additional information. (*See* **Section VIII Breach Notification Procedures**).

- If possible, determine what might prevent a similar breach, in the future. If lax firewall rules allowed the breach, tighten the firewall rules. If lax security practices allowed the breach (e.g. allowing remote "root" or "Administrator" logins), institute policies that disallow those practices.

VIII. Breach Notification Procedures

Allegiance shall notify a client group health plan following discovery and without unreasonable delay but in no event later than twenty (20) calendar days following discovery of any "Breach" of "Unsecured Protected Health Information" as these terms are defined by the HITECH Act and its implementing regulations. The Allegiance Privacy Official must be notified immediately of all known breaches or potential breaches to which any employee becomes aware. Allegiance shall cooperate with client group health plan in investigating the Breach and in meeting client group health plan's obligations under the HITECH Act.
When PHI is used or disclosed in violation of the privacy rule, a risk assessment must be performed to determine whether breach notification is required. The breach notification rules effective September 23, 2013 presume that notification is required, unless a formal risk assessment demonstrates that there is a "low probability" that the PHI has been compromised..

Allegiance shall follow its notification requirements outlined immediately below for purposes of detecting, containing and correcting any Breach.

a. For Successful Security Incidents and any other use or disclosure of PHI not permitted by the Agreement, the separate agreement, applicable law, or without the written approval of the Covered Entity, Business Associate,-- without unreasonable delay and in no event later than thirty (30) days after Business Associate learns of such non permitted use or disclosure—shall provide client group health plan a report that will:

    1. Identify (if known) each individual whose Unsecured PHI has been or is reasonably believed by Business Associate to have been accessed, acquired, or disclosed during such Breach;

    2. Identify the nature of the non-permitted access, use, or disclosure including the date of the incident and the date of discovery;

    3. Identify the nature and extent of the PHI accessed, used, or disclosed (e.g. name, DOB, whether it is sensitive nature such as diagnosis or treatment information creating a risk of identity theft);

    4. Identify who made the non-permitted access, use or received the non-permitted disclosure and whether the recipient has an obligation to protect the confidentiality of the PHI and whether the PHI was actually acquired or viewed by the unauthorized person;

    5. Identify the corrective action Allegiance took or will take to prevent further non-permitted accesses;

    6. Identify the corrective action Allegiance took or will take to prevent further non-permitted accesses, uses or disclosures;

    7. The extent to which the risk has been mitigated (for example, if the unintended recipients return or destroy the PHI);

    8. Identify what Allegiance did or will do to mitigate any deleterious effect of the non-permitted access, use or disclosure; and,

    9. Provide any other information the client group health plan may reasonably request.

b. For Unsuccessful Security Incidents, that is, incident that do not result in unauthorized access, use, disclosure, modification, or destruction of client group health plan's PHI, Allegiance shall provide client group

health plan, upon its written request, a report that: (i). identifies the categories of Unsuccessful Security Incidents; (ii) indicates whether Allegiance believes its current defensive security measures are adequate to address all Unsuccessful Security Incidents, given the scope and nature of such attempts; and (iii) if security measures are not adequate, the measures Allegiance will implement to address the security inadequacies.

GENERAL POLICY STATEMENT REGARDING PROTECTED HEALTH INFORMATION

Allegiance will not disclose any protected health information (PHI) about clients' participants or former participants to anyone, except as permitted or required by law. Allegiance will only disclose PHI in de-identified form unless the disclosure:

- Is to the person who is the subject of the PHI;
- Cannot be disclosed in de-identified form and is necessary for payment activities, healthcare operations, or plan administration.
- Is subject to a valid authorization; or
- Is permitted or required by law.

If health information cannot be provided in de-identified form, **we will only disclose the Minimum Necessary PHI for the stated purpose and only to an individual with a legitimate need to know** (in the case of the Plan, the designated Privacy Contact) **for payment activities, healthcare operations or plan administration.** Allegiance, on behalf of the client group health plan, will make reasonable efforts to limit PHI to the minimum necessary when (a) using PHI, (b) disclosing PHI, and (c) requesting PHI from a Covered Entity; unless Allegiance determines de-identified information is sufficient.

Allegiance will not be a party to disclosing or exchanging information under circumstances which would violate applicable privacy laws. In accordance with Allegiance's internal Privacy Policy, if the individual's valid authorization has not been provided, any request by a group health plan representative for PHI which has not been de-identified must be submitted in writing and the reason for requesting information in other than de-identified form must be stated. Allegiance retains the discretion to limit use or disclosure of PHI to de-identified form if it reasonably believes allowing access to or disclosing PHI could place Allegiance in violation of HIPAA.

GENERAL PROCEDURES FOR USE AND DISCLOSURE OF PHI

Flow of PHI

Although some departments will receive and handle PHI routinely, every department has the potential to receive and handle PHI. Examples items each department may receive include, but are not limited to:

- Accounting (PHI on large cases, plan reports)
- Flex (medical reports, medical claims, EOB's, medical info on reimbursement requests)
- Enrollment (health statements, information to determine pre-existing conditions, COBRA claims)
- Legal (reimbursements, claims overpayments, subrogation, appeals, legal action)
- Claims (claims, appeals, medical reports, EOB's)
- Customer Service (claims, medical reports, EOB's, requests for PHI)
- IT (accessing LuminX claim files or chronology for IT-related issues)
- Indexing (claims, appeals, medical reports)
- Mail/Scanning (claims, appeals, medical reports, EOB's)
- Administration/Marketing (PHI on stop-loss cases for submitting quotes to stop-loss carriers)
- Provider Services (pharmacy records, claims, EOB's)

Routine and Recurring Disclosures

Some disclosures of PHI are made on a routine and recurring basis to individuals with a legitimate need to know for purposes of payment activities or healthcare operations. The following individuals have a legitimate need to receive PHI for the specified

circumstance. Allegiance will limit the PHI disclosed to the **minimum amount necessary** to achieve the purpose of the disclosure to these individuals for these circumstances:

- **Allegiance**, as the third-party administrator and claims payor, has access to all PHI information available to the Plan Administrator, in order to perform its duties, as follows:
    - **Claims and Appeals.** Plan Administrator, or designated Plan Fiduciaries, with discretion to review claims decisions and/or claims appeals, may use or disclose that amount of PHI, as necessary in their discretion and professional judgment, to render a claims determination or decide an appeal.
    - **Eligibility.** Plan Administrator, or designated Plan Fiduciaries, with discretion to review eligibility decisions, has access to all enrollment information of Plan participants and those individuals who have applied for coverage under the Plan.
    - **Coverage.** To determine coverage, the Plan Administrator, or designated Plan Fiduciaries with discretion to review claims decisions and/or claims appeals, shall have access to the individual's claims file regarding the claim in question.
    - **Coordination of Benefits.** To coordinate benefits, the Plan Administrator, or designated Plan Fiduciaries has access to all enrollment information on those Plan participants subject to the inquiry, as well as information on other coverage those participants may have.
- **Privacy Official and Designated Staff.** The Privacy Official and designated staff shall have access to information regarding claims filed, appeals filed, eligibility, enrollment, termination, COBRA coverage and applications for coverage, as necessary to supervise the day-to-day operations of the Plan and to assist participants with questions and concerns regarding their benefits under the Plan.
- **Plan Auditor(s).** Plan Auditor(s) shall have information regarding claims filed, PPO repricing, claims paid, stop-loss submittals, eligibility, enrollment, termination, COBRA participants, COBRA premiums, participant contributions *and checking accounts* to audit the handling of funds related to the Plan as well as Plan assets.
- **Plan Operations.** Plan Administrator, or designated Plan Fiduciaries shall have access to all information needed to oversee and make decisions concerning Plan Operations, including claims costs, administrative costs, stop-loss premiums and provisions and audit reports.
- **Chief Financial Officer.** Chief Financial Officer(s) of Plan Sponsor and Plan Administrator shall have access to all information regarding funding and expenses of the Plan, including but not limited to, information regarding claims filed, PPO repricing, claim funding requirements, claims paid, stop-loss submittals, COBRA premiums, participant contributions and checking accounts.
- **Plan Sponsor Audits.** For auditing purposes, the Plan Sponsor shall have access to claims information for the prior plan year, as well as information regarding specific claims as are requested to assess the Plan's performance and review Plan costs.
- **Underwriting.** For underwriting purposes, the stop-loss carriers and managing general underwriters from whom quotes are obtained shall have access to aggregate claims information for the prior plan year, as well as such information regarding specific claims as requested to determine the cause of unexpected claims that could influence the premium; however, whenever possible, information shall be provided in de-identified form.
- **Stop Loss Claims.** The stop-loss carrier and managing general underwriter shall have access to information regarding specific and aggregate claims as necessary to determine whether or not such claims are payable or reimbursable.
- **Personal Representatives.** Personal representatives shall have access only to that individual's PHI relevant to the purpose of their appointment if the personal representative was appointed for a limited purpose. (For example, if a personal representative is appointed solely to make decisions regarding an individual's cancer treatment, the personal representative shall have access only to the individual's PHI relating to cancer treatment.) Allegiance must receive prior written authorization and supporting documentation establishing the authority of the person to act as a personal representative.
- **Utilization Review Companies.** Any utilization companies used by the Plan shall have access to such medical records and

medical information as necessary to perform their duties related to pre-admission certification subject to the terms of the Business Associate Agreement between the utilization company(s) and the Plan.

- **Case Management Companies.** The applicable case manager of the case management company(s) used by the Plan shall have access to such medical records and medical information relevant to individuals for whom they perform case management services as necessary to perform their duties, subject to the terms of the Business Associate Agreement between the case management company(s) and the Plan.

- **Attorney(s).** For purposes of providing legal services to the Plan, the Plan's attorneys shall have access only to that individual's PHI related to issues on which the attorneys advise the Plan.

- **Broker(s).** For purposes of providing advice to the Plan, its broker shall have access to such eligibility, enrollment, termination, COBRA, claims and stop-loss information as necessary to provide accurate and complete advice, subject to terms of the Business Associate Agreement between the broker and the Plan.

- **Subrogation Vendor, if this function is outsourced.** Any subrogation vendor shall have access to such medical records, accident information and claims information as necessary to perform its duties relating to the Plan's subrogation interests, subject to the terms of the Business Associate Agreement between the subrogation vendor and the Plan.

- **COBRA Vendor, if this function is outsourced.** Any vendor used by the Plan to provide COBRA administration services shall have access to such information relating to enrollment, eligibility, termination, COBRA elections and payment of COBRA premiums as necessary to perform its duties for the Plan, subject to the terms of the Business Associate Agreement between the COBRA vendor and the Plan.

- **Preferred Provider Organization or other Managed Care Organization.** Any preferred provider organizations providing discounted rates to the Plan has access to all claims relating to services provided by member providers for re-pricing of claims and resolution of any related disputes.

- **Printing and Mailing Services.** Any printing and mailing service used by the Plan has access to those documents to be printed and mailed.

- **Scanning and Scrubbing Services.** Any scanning and/or claims "scrubbing" service(s) used by the Plan shall have access to the documents to be scanned and the Plan's database.

- **All other Disclosures.** For all other disclosures, the Privacy Official shall review each request for disclosure in accordance with the Privacy Team's established criteria and any directives from the Plan Administrator. The Privacy Official may also consult with the requesting party, as necessary, to determine the purpose of the requested disclosure. As necessary, the Privacy Official may utilize appropriate professionals to determine the minimum necessary disclosure of PHI.

- **Request for Entire Medical Record.** Any use or disclosure of, or request for, an individual's entire medical record shall be examined by the Privacy Officer in consultation with the Plan Administrator, who shall determine, in its discretion, whether the use, disclosure or request is specifically justified as that reasonably necessary to accomplish the purpose of the use, disclosure or request. If necessary, the Plan Administrator shall consult appropriate professionals to assist in determining whether the use, disclosure or request is justified.

Privacy Contact(s) for Group Health Plans

Because client companies have dual roles as an employer and as Plan Sponsor of a group health plan, we limit disclosure of PHI to the group representative to situations in the client's role as Plan Sponsor for plan administration purposes. As a procedural safeguard, the Legal Department sends client companies a contact form in which the Plan Sponsor designates the person(s) authorized to receive PHI for plan administration purposes, such as plan funding, forecasting claim liability and obtaining stop-loss coverage. Calling on behalf of employees to assist with claims issues or seeking personal medical information about employees or their dependents are not plan administration functions; accordingly, for this purpose, PHI on employees and their dependents can only be provided to the Plan Sponsor or group health plan representative with the individual's valid authorization.

These charts are posted in Adobe (a separate topic called "Privacy Contacts" following "Claims Forms") and updated periodically. Use the chart to note the contact(s) for the group(s) you work with.

Any time you are asked to discuss or exchange personal medical information with the group for plan operations, use only the contact(s) shown. If you are asked to provide PHI to another individual on behalf of the group, or if you have any questions about the

group privacy contact information, please contact the Privacy Official in the Legal Department.

ALLEGIANCE CANNOT DISCLOSE PHI FOR PAYMENT, HEALTHCARE OPERATIONS OR PLAN ADMINISTRATION FUNCTIONS UNTIL A COMPLETED AND SIGNED PRIVACY CONTACT FORM IS RECEIVED. UNTIL THAT FORM IS RECEIVED, HEALTH INFORMATION CAN ONLY BE DISCLOSED IN DE-IDENTIFIED FORM.

Use and Disclosure of PHI by Allegiance (on behalf of the Plan)

Without Valid Authorization: Allegiance will only disclose PHI without a valid authorization in the following instances:

- To the individual for whom the PHI pertains (or to a minor child's parent or guardian or the individual's personal representative if the individual is incapacitated) under the individual's right to inspect or copy;
- As required for healthcare operations purposes; or
- As required for payment purposes; or
- As required for plan administration functions; or
- As required or permitted by law. [See Appendix B, Notice of Privacy Practices, for list of disclosures Allegiance may make.]

With Valid Authorization: Any other uses and disclosures not specifically described above will be made only with the individual's (or the individual's guardian or parent, if a minor) valid authorization. [See Appendix C for Authorization form.]

- Authorization is effective until the individual is no longer covered under the group health plan or for two years, whichever occurs first, or the individual revokes the authorization in writing.
- An individual may revoke his or her written authorization at any time, by sending written notice to Allegiance.
- Written revocation may not be effective, if Allegiance has already released the PHI, or that authorization was a condition of the individual's enrollment in the Plan.
- PHI may be disclosed with valid authorization on file, even though Allegiance later receives a written revocation.
- PHI may not be released to spouses or parents of dependent children who are not minors (or emancipated minors) without valid authorization – even if the spouse or parent is a plan participant.
- Valid authorization from the individual should state who the Plan may discuss PHI with (such as the spouse, parent, or other party, **including the employer or group plan representative**). Employers cannot use PHI to make employment decisions, unless the individual gives valid authorization.

Mental health information may not be disclosed, even to the individual, without consent of the treating provider.

General Compliance Procedures for Releasing PHI

Disclose the minimum amount of PHI necessary for the stated purpose. Allegiance will provide PHI in de-identified form whenever possible, unless the disclosure is to a treating provider for treatment, made to the individual pursuant to valid authorization, or made to appropriate government authorities, required by law or required for compliance with HIPAA.

Effective April 14, 2003, monthly reports and information necessary for payment or healthcare operations will be provided in de-identified form. Usually, Plan Administrators and stop-loss carriers need to know only that a claim for a particular condition exists to determine stop-loss rates or forecast liability for a particular condition; they generally do not need the individual's name or any information identifying that individual in order to determine stop-loss rates or forecast plan liability.

De-identified form means data that identifies the individual has been removed, such as name, address, dates like the individual's birth date, phone numbers, or social security number has been removed.

Note any restrictions the individual has requested. The individual has the right to request that Allegiance limit how it uses or discloses the individual's PHI, as well as how much of and to whom the individual's PHI may be disclosed. This includes disclosures to family members, relatives, close personal friends or other involved persons. The individual may also request that Allegiance communicate with them in a certain way or at a certain location. For example, that individual may ask that Allegiance only communicate with them at their place of work or by mail. The individual may also have requested that their spouse or that the named subscriber on their group health plan, for example, not receive any of their PHI.

- A request to restrict use and disclosure must be in writing and addressed to the Privacy Official, who determines whether or not to grant the request(s).
- Request should include what information the individual wants restricted; whether the individual wants to restrict use, disclosure, or both; and to whom these restrictions should apply.

- If the request is granted, Allegiance will maintain a record of the restriction and record in the "Remarks" section of chronolog. Once they receive notice of a granted request, Enrollment department employees will make these entries.
    - Records of restrictions to be retained for 6 years from date of entry or date last in effect, whichever is later.
    - Allegiance must honor a restriction it agrees to, except when the individual needs emergency care and the PHI is necessary for health care providers to provide emergency care to the individual. If restricted PHI is disclosed for emergency treatment, Allegiance may ask the health care provider to not use or disclose the PHI for any other purpose.
- Allegiance does not need to agree to a requested restriction.
- Allegiance can terminate an agreement to restrict use or disclosure if:
    - Individual agrees to or requests the termination either orally or in writing;
    - Allegiance notifies the individual of its intent to terminate the agreement. This termination affects only that PHI created or received after the date the individual is notified.
- An individual may ask to receive his or her PHI confidentially and Allegiance may accommodate the individual's request, within reason. This may include for example, a request to communicate with the individual only at work, or by mail.

Verify identity of the person or entity requesting PHI and authority of that person or entity to have access to PHI, if you do not know the person (or entity).

- **Verify identity** by requesting a medical provider's employer identification number (EIN) when the provider requests PHI or an individual's Social Security Number when the individual requests PHI. If state law does not permit use of Social Security numbers, then use another unique item of information (home address, mother's maiden name, name of primary care physician). You may also rely upon, in the following order:
    - Written statement of legal authority, such as a power of attorney, personal representative or guardianship;
    - Oral statement, if a written statement is impracticable;
    - Warrant, subpoena, court order or other similar legal process.
- **Identity and Authority of Public Officials:** Rely, if reasonable, on the following to verify the identity of a public official (or someone acting on behalf of a public official) and that person's authority to act:
    - Agency identification badge, other official credentials or proof of government status;
    - Appropriate government letterhead, if the request is made in writing;
    - Written statement on government letterhead that the person is acting under government authority or other, such as a contract for services, memorandum of understanding or purchase order, establishing the person's identity and authority to act, if the request is made by someone acting on behalf of a public official.
    - A warrant, subpoena, order or other similar legal process.
- **Get copies** of the consent, authorization, proof of personal representation, power of attorney and other appropriate documentation before disclosing PHI. You may rely, if reasonable, on documentation that appears valid.
- **Exceptions to Verification Procedures.** Verification is not required for:
    - Disclosure to family member, other relative or close personal friend, or to any other person identified by the individual, if the PHI is directly related to that person's involvement with the individual's health care (or payment of); or
    - Disclosure to notify (or identify or locate) a family member, a personal representative of the individual or another person responsible for the care of the individual, of the individual's location, general condition or death. Here, the Plan Administrator (or Sponsor), or the Privacy Officer may use its professional judgment to review requests for disclosure.

Penalties for Disclosing PHI in Violation of HIPAA

In addition to employment sanctions and criminal penalties, as amended by the HITECH Act, financial penalties for wrongful disclosures may be as high as 1.5 million dollars in one calendar year.

THESE PENALTIES CAN APPLY TO THE INDIVIDUAL AND THE INDIVIDUAL'S EMPLOYER.

Allegiance employees may also be subject to disciplinary action, up to and including termination of employment, for violations of an individual's right to privacy under HIPAA regulations.

Plan Sponsor Access to PHI

The Plan Sponsor is typically the employer. Allegiance may disclose PHI to the Plan Sponsor/Employer for plan administration, if the Plan Sponsor certifies that Plan Documents have been amended by incorporating the following provisions. Plan Sponsor/Employer must agree to:

1. Not use or further disclose PHI other than as permitted or required by Plan Documents or as required by law;
2. Ensure that any employees or subcontractors, to whom it provides PHI received from the Plan, agree to the same restrictions and conditions that the Plan Sponsor must follow;
3. Not use or disclose the PHI for employment-related actions and decisions of the Plan Sponsor;
4. Report to the Plan any known use or disclosure of PHI inconsistent with permitted uses or disclosures;
5. Allow an individual to inspect or get a copy of his or her PHI as permitted by HIPAA;
6. Allow the individual to amend his or her PHI and incorporate any amendments into PHI as required and permitted by HIPAA;
7. Give the individual an accounting of disclosures made of his or her PHI, as requested;
8. Make its internal practices, books, and records relating to the use and disclosure of PHI received from the Plan available to any applicable regulatory authority to determine the Plan's compliance with HIPAA;
9. If feasible, return or destroy all PHI received from the Plan that the Plan Sponsor still maintains in any form and keep no copies of PHI when no longer needed, except that, if this is impossible, limit further uses and disclosures to those purposes that make the return or destruction of the information impossible; and;
10. Ensure adequate separation between the Plan and Plan Sponsor. Access to PHI will be restricted to those employees, classes of employees or other persons who need access to that PHI to perform plan administration functions. Plan Sponsor will maintain appropriate safeguards and develop policies, as necessary, to protect the confidentiality of PHI and will provide only the minimum PHI necessary for plan administration.

Allegiance is a contract claims payer for its client group health plans and has Business Associate Agreements with all client group health plans, with an obligation to meet the above Plan Sponsor requirements.

ANY DISLOSURE OF PHI NOT SPECIFICALLY PERMITTED BY THESE PRIVACY POLICIES AND PROCEDURES IS A PROHIBITED DISCLOSURE FOR ALLEGIANCE EMPLOYEES.

Maintaining a Disclosure Log

Allegiance is required to maintain a record of PHI disclosures for auditing purposes. The log need not include disclosures permitted without valid authorization or made prior to April 14, 2003. The Privacy Official will maintain this log. The log shall be maintained in an electronic sub-file of LuminX designated as "DL". Except for disclosures set forth in §164.528 (a)(1), of the Privacy Regulation, an individual may request a listing of those persons or organizations to which Allegiance disclosed the individual's PHI:

- Request must be in writing and addressed to the Privacy Official.
- Individual to get one free listing per year; all others may be subject to a reasonable fee.
    - Fee is **15 cents per page, plus $15.00 for handling**.
- Listing of disclosures to include:
    - Disclosures made within 6 years of date of request unless the individual asks for a shorter time;
    - For each disclosure, date, recipient, brief description of PHI disclosed & reason for disclosure.

Individual's Right to Complain

Individuals may file a complaint if they believe their privacy rights have been violated. Any complaint filed must be in writing and may be submitted to the addresses as noted in the Notice of Privacy Practices on Allegiance's website or available in paper copy from the Plan representative or Allegiance. [See Appendix B for a copy of the Notice.]

- Any correspondence or questions received by Allegiance alleging a violation of the individual's privacy rights will be directed to the Privacy Official for handling.
    - The Privacy Official (or Privacy Team) may investigate and cure, as appropriate, any alleged violation.

- Privacy Official may notify the Plan Administrator or Plan Sponsor, if different, of the alleged privacy violation.
- Allegiance will mitigate, as much as reasonably practicable, effects of any known breach of an individual's privacy rights.

PRIVACY TRAINING MANUAL

The Privacy Training Manual may help you field questions from both claimants and group representatives concerning the new privacy regulations. The Manual provides answers to questions which may be asked of you. The Manual will be updated periodically to include additional information on frequently asked questions.

POLICY FOR DISCUSSING AND RELEASING PHI ON THE TELEPHONE

Allegiance will not release PHI on the telephone unless:

- Requested PHI pertains to the caller and you have adequately verified the caller's identity; or
- A written request for a specific purpose has been provided; Allegiance has confirmed that the purpose is legitimate; and disclosure is to an authorized Privacy Contact(s); or
- Allegiance has a valid authorization on file;
- The individual's health information has been de-identified.

After verification, Allegiance will only release the minimum necessary PHI for the stated purpose.

PROCEDURES AND GUIDELINES FOR TELEPHONE CALLS

General Policy Statement

Unauthorized disclosure of PHI creates significant liability both for Allegiance and for the person making the disclosure. If there is question whether or not to disclose PHI, either contact the Legal Department or take the conservative approach –"if in doubt, don't give it out."

The privacy requirements may be inconvenient and frustrating for customers and client companies. It may be difficult for plan representatives trying to help employees/claimants resolve a problem to understand why now, we need valid authorization from the claimant before we can disclose information we may have given freely in the past. Every effort will be made to provide customers and plan representatives with information they need. HIPAA is applicable to all companies, not just Allegiance.

Focus on what can be done for the caller. Confidential information can be provided with a valid authorization form. The authorization forms can be downloaded from our website (www.abpmtpa.com) or accessed via the group health plan representative. If the caller does not have access to the Internet or cannot get an authorization form from the group health plan representative, mail an authorization form to the caller.

Phone Disclaimer for Incoming Calls to Allegiance

Federal privacy laws require all companies, including Allegiance, to get valid authorization, before disclosing an individual's confidential health information to a third party. This applies to everyone. For example, health information of spouses and dependent children who are not minors cannot generally be disclosed without their authorization, even to their spouse or parent absent. If you have a question concerning health information on someone besides yourself, we need valid authorization from that person before we can give this information to you. Authorization forms are available on our website (www.abpmtpa.com) or from your group health plan representative. We understand these new requirements may be inconvenient for you. Please understand that we are required by law to follow them. When we receive the completed form, we will keep a record of those persons you have authorized us to discuss your confidential information with and any restrictions on what we can discuss, so that you do not need to sign a new authorization each time you call.

Disclaimer to be Read to Claimant Prior to Discussing PHI Via Conference Call or Speaker Phone

"(Name), in order for me to [help you/answer your question(s)], I may need to talk about specific details of your [medical care/treatment/doctor visit/etc.] which most people would consider confidential information. Before we start,

I need to tell you that the new federal privacy regulations allow you to keep your medical information private and not to disclose it to anyone else except in certain limited situations. You are not required to discuss your confidential medical information with anyone else [present/on the line/involved] unless you want to. It is your choice. If you want to discuss this matter with [employer representative/name of person] present, we can continue now. If you prefer, you can call me back at another time or from another phone (give #). What would you like to do?

Note General Compliance Procedures on page 10 – verifying the identity of the caller, if the caller is someone other than the individual, and noting any restrictions the individual may have placed on disclosure of his or her PHI.

POLICY FOR SENDING OUT PHI VIA MAIL OR FAX

Allegiance will only release PHI via fax in accordance with guidelines in this Privacy Training Manual.

PROCEDURE FOR SENDING OUT PHI VIA MAIL OR FAX

EXAMPLE: Suppose a Plan Administrator asks for copies of claims information because they were doing an "audit" on an employee's claims. A plan audit is a plan administration function for which we can release PHI to the Plan Administrator or its designee without the individual's written authorization.

Suppose further, that this "audit" is not for plan administration purposes, but rather for an in-house investigation of the employee for alleged misconduct. Allegiance cannot provide the individual's PHI to his employer for this purpose without the individual's written authorization.

- Non-Routine Requests for Claims Information on an Individual:
    - When a Plan representative requests an enrollee's claims information, which is PHI, send either by fax or mail, the Request for Information Form (see Appendix F) to determine the reasons for the request.
    - When the completed form is received, refer it to the Privacy Official (or Privacy Team) for review and approval.
    - Once approved, the requested PHI may be sent to the Plan Representative.
    - If not approved, the Privacy Official (or Privacy Team) may either ask you to get valid authorization from the individual to disclose the information; or the Privacy Official (or Privacy Team) may notify the Plan representative in writing why the PHI will not be sent.
- Routine Monthly Reports
    - All report requests for group information should be routed through the Claims Manager (Gary Ritter) for approval.
    - If approved, the report will be processed and sent.
    - If not approved due to limitations of the system, the Claims Manager will determine which reports can be run to provide the requested information.
    - If the report cannot be run for other reasons, the Claims Manager may notify you what is needed to run the report. This may include obtaining valid authorization from the individual.
    - If a report cannot be sent as requested, (if at all), the Privacy and Compliance Official will send the Plan Administrator notice of this in writing.
- Fax Requests
    - If someone requests that PHI be sent by fax, then fax only if:
        - You confirm that recipient has a secured fax machine, or
        - The recipient will wait to personally receive it.

- Confidentiality Notice: The current version of the Confidentiality Notice should be sent out with any PHI, plan reports containing PHI, and any other information proprietary to Allegiance. See Appendix E.

POLICY REGARDING DESIGNATED RECORD SETS

Allegiance will create and maintain Designated Record Sets for all individuals covered under those plans for which Allegiance provides benefits management services. The designated record set will be stored electronically in LuminX.

What is a Designated Record Set?

- A group of records maintained by Allegiance or for a client group health plan that includes:
  - Medical and billing records about individuals;
  - Enrollment, payment, or claims adjudication records, and/or:
  - Case or medical management record systems.

- Designated Record Set is not:

  - Chronolog notes maintained by Allegiance;
  - Internal memos of the Plan Administrator or Allegiance;
  - Information created or obtained in anticipation of some legal proceeding;
  - Any privileged or proprietary information of the Plan or Allegiance.

POLICY FOR AN INDIVIDUAL'S RIGHT TO ACCESS OR AMEND HIS OR HER PHI

Allegiance will give individuals the right to inspect or get a copy of the PHI in their Designated Record Set and permit them to amend and/or append the PHI in their Designated Record Set, subject to applicable limitations and restrictions.

PROCEDURES REGARDING THE RIGHT TO ACCESS, AMEND OR APPEND PHI

Notice of Privacy Practices is given to enrollees of the client group health plans and explains their rights with regard to their PHI. See Appendix B.

Right to Inspect or Copy PHI - Procedure

- Requests by the individual must be in writing and addressed to the Privacy Official;
- The request must be processed within 30 days after receiving the request by either providing access to the PHI or a letter stating why access will not be provided.
  - If the request is granted:
    - And the PHI is not maintained or accessible to Allegiance on-site, Allegiance may have up to 60 days;
    - And Allegiance cannot provide access within those 30 or 60 days, it may have an additional 30 days, if it notifies the individual in writing of the reason for the delay within that initial 30 or 60 days; or
    - If the individual asks for a photocopy or summary of his or her PHI, the individual will be responsible for reasonable costs to copy, mail, or prepare the information.
      - Fee is **15 cents per page, plus $15.00 for handling.**
  - If the request is denied:
    - Because Allegiance does not maintain the PHI onsite, Allegiance must tell the individual who maintains his or her PHI;
    - The individual may, in some cases, have his or her denial of access reviewed by a health care professional under contract with Allegiance, who was not involved in the earlier decision to deny access.
- If someone other than the individual him or herself asks to inspect the individual's PHI in person, note the General Compliance Procedures on page 10 - verifying the identity of the caller, if the caller is someone other than the individual, and noting any restrictions the individual may have placed on disclosure of his or her PHI.

When can access to either inspect or copy PHI be denied?

An individual may be denied access if:

- PHI is psychotherapy notes;
- PHI is information gathered in anticipation of a legal action or proceeding,
- PHI is lab information subject to federal regulations that prohibit disclosure;
- PHI relates to a correctional facility inmate's request;
- PHI is obtained by a covered health care provider during research including treatment;
- Allowing access to PHI would reveal the identity of the confidential source who provided the PHI;
- Allowing access to PHI might endanger the life or health of the individual or another person referenced in the PHI.

Right to Amend or Append PHI

An individual may ask Allegiance to amend his/her PHI in a designated record set for as long as the Plan (or Allegiance) maintains the PHI.

- Requests to amend should be in writing and addressed to the Privacy Official. Request should include a reason that supports the request;
- Requests must be acted upon within 60 days of receipt. If Allegiance cannot act within 60 days, it has 30 more days, IF it notifies the individual in writing of the reason for the delay within those 60 days.
- If the request is granted, Allegiance must amend the individual's PHI, promptly notify the individual and get from him or her, the names of other persons who need to know about the amended PHI. Allegiance must notify those persons and any others that it knows has a copy of the individual's PHI and may have used or might use that PHI.
- If the request is denied, Allegiance will notify the individual in writing and include the reason why.
    - If the individual disagrees, he or she can make a written statement of disagreement. Allegiance may prepare a written rebuttal to this statement and forward a copy to the individual. Both the statement and rebuttal to be incorporated into future disclosures of the PHI.

Reasons to Deny the Right to Amend or Append PHI

Allegiance may deny an individual's request to amend his/her PHI if the PHI:

- Was not created by the Plan, unless the individual proves that the originator of his or her PHI is no longer available to act on the amendment;
- Is not part of the Plan's designated record set;
- Is not available for the individual to inspect; or
- Is accurate and complete.

PROCEDURES REGARDING SECURITY AND ADMINISTRATIVE SAFEGUARDS FOR PRIVACY

Disposing the Original Documents

Once scanned, original documents are stored in a secure, locked area for at least 6 years and subsequently shredded or returned to client(s), as appropriate.

Physical Safeguards

Work Stations

- Keep work stations clear of visible PHI.
- Work stations for claims examiners will be in a secure location behind a locked door with an access code, accessible only to employees.
- Originals of legal documents are stored in secured fireproof file cabinets in Legal Department.
- Copies of PHI should not routinely be kept at work stations, unless for the following:
    - Prepared for the Quality Assurance Supervisor to respond to appeals;
    - Prepared for Legal Department for collection of claims overpayments;
    - Prepared for Legal Department for subrogation/reimbursement activities.

Computer Terminals

To prevent unauthorized access to PHI through the computer terminal, the following procedures have been implemented:

- Turn off computer monitors when leaving desk for breaks or lunch;
- Turn computers off at the end of the day;
- Position computer monitors on the desks to shield monitors from view of customers or clients.
- When computers are discarded or sent to storage, IT will clear hard drives of any data not required to be stored or retained;
- Screen savers will be installed on computers in high traffic areas and be set to activate after 3 minutes.

Disposing PHI
PHI no longer necessary will be shredded by Allegiance employees. All other documents to be shredded should be placed in locked "Tear It Up, Inc." dumpsters. Tear It Up, Inc. will shred these documents onsite. Tear It Up, Inc. shall be a Business Associate contractor of Allegiance.

Mailing PHI (i.e. EOB): No PHI should show through a window envelope. Ensure that the individual receives only his or her EOB.

Electronic Safeguards
IT Department will develop electronic safeguards and related policies, for approval by the Privacy and Compliance Official. Safeguards are in currently in place for electronic claims submission and storage and retrieval of electronic information. Access to electronic PHI is allowed on a legitimate need to know basis and limited to the minimum necessary for the purpose. PHI is generally stored on the mainframe and accessible only through individual sign-on and password.

Both incoming and outgoing telephone calls are recorded.

Procedural Safeguards
All employees must maintain the confidentiality of PHI and follow Allegiance's Privacy Policies and Procedures. Specific procedures include:

- Reference checks for new employees;
- Ongoing employee training on privacy policies and procedures;
- Ongoing internal audits to determine additional internal compliance procedures necessary;
- PHI is proprietary to Allegiance and unauthorized or inappropriate use or disclosure of PHI may subject the employee to disciplinary action, up to and including immediate termination.

POLICY FOR VISITORS AND VENDORS

All visitors, including any vendors, to any Allegiance building, must sign in and out of the building using the Visitor Log located in the reception area. The visitor shall be issued a visitor identification badge to be prominently displayed by the visitor at all times while onsite. Visitors shall not be granted access behind any of the buildings' doors having a key swipe door lock unless absolutely necessary to perform a particular function or service a particular piece of equipment. At all times the visitor must be escorted by appropriate Allegiance personnel in any area where PHI is being stored or used.

POLICY FOR WEBSITE ISSUES AND ACCESS

Allegiance will maintain a secure and HIPAA-compliant website, providing limited access to PHI by Covered Persons and Providers.

PROCEDURES FOR WEBSITE ISSUES AND ACCESS

General Information About the Website

Allegiance will implement appropriate electronic, procedural and physical safeguards, including but not limited to Personal Identification Codes, the System Usage Conditions and Systems Usage Agreement, as now written or subsequently revised or amended, to comply with all applicable privacy and security laws; **however, Allegiance will have no liability for outdated information on its website which may result from untimely notice by Plan Administrator(s) of revisions or changes to the Plan.**

Allegiance will host a secure, interactive website with access to claims, eligibility, and benefit information for individuals covered under our client companies' group health plans. The information available to the Plan and covered enrollees is limited to that of the applicable group health plan(s) only or to information available to the general public.

The interactive website can be used to check benefit information and track claims payment status. The website information can only be accessed through the use of a Personal Identification Code (PIC) issued directly to the covered participant. The PIC allows the individual to access information concerning the eligibility, plan coverage, and deductible for the individual participant and any covered family members.

The information available to covered individuals via the website does not replace any legal notice requirements the Plan Administrator has with regard to group health plans. The Plan Administrator(s) will continue to timely provide and distribute all required notices and information to Participants.

If there is a discrepancy between the information accessed via Allegiance's website and provisions of the Plan(s), then Plan provisions, as stated in the most-recently executed copy of the written Plan Document on file will prevail.

Allegiance will actively monitor both website access and other requests for PHI from individuals other than the person who is the subject of the PHI to assure that appropriate written authorization is provided to Allegiance or the Plan, as applicable, or that PHI is being disclosed for legitimate plan administration purposes. If Allegiance knows of unauthorized use or disclosure of PHI, Allegiance will take immediate steps to mitigate any harm caused by such unauthorized use or disclosure. Such steps may include, but are not limited to, notifying the appropriate law enforcement authorities, the Office of Civil Rights and/or the Plan Administrator(s) of the affected group health plans.

Website Information – Covered Person

If Allegiance receives a completed online application request from a participant, he or she will be mailed a Personal Identification Code (PIC) to allow access to information concerning the eligibility, plan coverage, and deductible for the Participant and any covered family members on the website. A letter will also be sent to the individual to verify that the identity of the person requesting a PIC.

When first logging in, the individual must acknowledge the terms of the following Agreement:

SYSTEMS USAGE CONDITIONS

Claims Information available through the interactive website by use of your PIC is subject to the following conditions:

- Access to the website and claims information is accessible only by a Personal Identification Code which Allegiance Benefit Plan Management, Inc., will mail to a participant upon request;
- Access is restricted to information for the specific patient or patients covered through the applicable participant identification number;
- All information on the website is proprietary to Allegiance Benefit Plan Management, Inc., and all such information is confidential;
- Accessing or attempting to access information or programming in the system not specifically and directly part of the participant file(s) for the participant or family member(s) of the participant is expressly prohibited without qualification;
- The system contains safeguards and audit functions to detect unauthorized attempts to access and unauthorized access to the system;
- Any unauthorized access or attempt to access the system by a representative of a participant will result in immediate termination of all rights to access the system by the participant and any of the participant's covered family members;
- Any unauthorized access or attempt to access the system may result in the matter being reported to appropriate state or federal authorities for investigation and prosecution for violation of applicable privacy laws.

SYSTEMS USAGE AGREEMENT

Under Allegiance's website access policy and applicable federal and state privacy regulations, when you use your PIC and access Claims Information through Allegiance's website you agree to accept the following terms and restrictions:

- To access only your records;
- To safeguard your access code and share it only with a designated family member or members with a legitimate need to access their confidential Claims Information;
- To report any unauthorized access or security breach;
- To change, or request that Allegiance change your access code if you have reason to believe your existing access code has been appropriated by an unauthorized individual;
- Not to use this information in any manner that could result in the person who is the subject of the information from being denied any employment opportunities or having employment terminated.

The person who accesses Claims Information through this website, personally and/or on behalf of any family member, understands that the Claims Information is confidential and should not be disclosed in any manner, to any person or entity, except as required for legitimate plan administration purposes. The person receiving Claims Information through the website must protect the confidentiality of any PHI. Any person who receives Claims Information and believes he or she cannot abide by the terms of this notice should not access the website.

ANYONE LOGGING ON TO THE SYSTEM WILL BE DEEMED TO HAVE ACKOWLEDGED AND AGREED TO ALL TERMS

AND CONDITIONS STATED ABOVE.

Website Information - Provider

Health care providers may access Claims Information on the website for the limited purposes of payment activities, health care operations or plan administration functions. Upon request, providers will be issued a PIC in the same manner as to individual participants. The website provides Claims Information based on the provider's tax identification number (TIN). A provider's PIC may provide access to Claims Information of the patients of all providers who bill under that same TIN.

PHI accessible through the website for payment activities, healthcare operations or plan administration functions may not be used or disclosed by the provider for other purposes without valid authorization from the claimant.

When a provider first logs in to the website, he or she must read and acknowledge the following Systems Usage Agreement:

SYSTEMS USAGE CONDITIONS AND AGREEMENT

Claims Information available through the website with your PIC is subject to the following conditions and restrictions:

- Access to the website and claims information is accessible only by a Personal Identification Code which Allegiance Benefit Plan Management, Inc., will mail to a participant upon request;
- Access is restricted to Claims Information for specific patient(s) that the provider has or is providing treatment, services, or supplies to, and for no other information.
- All information on the website is proprietary to Allegiance Benefit Plan Management, Inc., and all such information is confidential.
- Accessing or attempting to access information or programming in the system not specifically and directly part of the patient file(s) for patients of the provider gaining access is expressly prohibited without qualification;
- The system contains safeguards and audit functions to detect unauthorized attempts to access and unauthorized access to the system;
- Any unauthorized access or attempt to access the system by a representative of a provider will result in immediate termination of all rights to access the system by that provider, the provider's staff or the staff of the clinic or facility with whom the provider is affiliated;
- Any unauthorized access or attempt to access the system may result in the matter being reported to appropriate state or federal authorities for investigation and prosecution for violation of applicable privacy laws.

Under Allegiance's website access policy and applicable federal and state privacy regulations, when you use your PIC and access Claims Information through Allegiance's website you agree to accept the following terms and restrictions:

- To access only the records of patients for whom you provide treatment, services, or supplies;
- To designate an individual or individuals from your office to have your PIC and thereby access to confidential patient Claims Information available through this website;
- To safeguard your PIC and share only with designated individuals with a legitimate need to access patient Claims Information;
- To report any unauthorized access or security breach;
- To change, or request that Allegiance change your access code if you have reason to believe your existing access code has been appropriated by an unauthorized individual;
- To not disclose the Claims Information, or any portion of it, in any manner likely to, or that does in fact, reveal the identity of any person named in the Claims Information to any person or entity, except those individuals who are expressly authorized to access for payment activities, healthcare operations, or plan administration functions;
- Not to use this information in any manner that could result in the person who is the subject of the information from being denied any employment opportunities or having employment terminated.

ANYONE LOGGING ON TO THE SYSTEM WILL BE DEEMED TO HAVE ACKOWLEDGED AND AGREED TO ALL TERMS AND CONDITIONS STATED ABOVE.

CLAIMS INFORMATION ACCESSED THROUGH THE WEBSITE IS NOT A GUARANTEE OF PAYMENT.

APPENDIX A

OVERVIEW OF PRIVACY POLICY

ALLEGIANCE BENEFIT PLAN MANAGEMENT, INC. AND INTERMOUNTAIN UNDERWRITERS, INC.

Federal laws, such as the Gramm-Leach-Bliley Act and the privacy regulations of the Health Insurance Portability and Accountability Act of 1996, as well as state privacy laws have been enacted to protect the use and disclosure of medical and financial information. These regulations restrict what information can be disclosed, to whom it can be disclosed and if authorization from the individual is necessary before such use or disclosure may occur.

Allegiance, as a third-party administrator, is not a covered entity as defined by these regulations. However, Allegiance has access to and receives individually identifiable health information to determine eligibility, adjudicate claims, and pay benefits for group health plans, which are covered entities subject to these regulations. Therefore, Allegiance has formally adopted this privacy policy, which is compliant with the requirements of applicable regulations under the Gramm-Leach-Bliley Act, HIPAA, and state privacy regulations.

GENERAL PRIVACY PROVISIONS

We, at Allegiance, value the trust our customers place in us and are dedicated to developing and maintaining their confidence in our products and services. In order to provide effective customer service and benefits management services, we must necessarily collect a certain amount of information. This privacy policy explains how we may collect information, what information we may collect, and what information we may disclose to nonaffiliated entities. We are committed to maintaining the confidentiality of customer information.

We may amend our privacy policies from time to time. We will notify our customers of any changes to our privacy policies. If our relationship with a customer ends, we will continue to limit use and disclosure of this information in accordance with our stated privacy policies.

Specific Safeguards to Protect Confidential Customer Information

Procedural Safeguards

All employees are accountable for, and required to maintain, the confidentiality of customer information and to follow Allegiance's privacy policies. New employees are subject to background reference checks to identify any past acts or activities which may create concern in entrusting the individual with, or providing the individual with access to, confidential customer information.

Allegiance conducts ongoing employee training on privacy compliance. Allegiance's employee handbook states that confidential customer information is proprietary to Allegiance and that unauthorized use or disclosure of such information may be grounds for disciplinary action, up to and including immediate termination.

Allegiance performs ongoing internal audits to determine what additional internal compliance procedures may be necessary to secure confidential customer information.

Electronic Safeguards

Allegiance has implemented safeguards with regard to electronic claims submission and the storage and retrieval of electronic customer information. Access to electronic customer information is allowed on a legitimate need to know basis and limited to the minimum necessary for the purpose. Electronic customer information is accessible only through individual sign-on and password. Access is designated to a limited number of individuals to handle paper claims.

Both incoming and outgoing telephone calls are recorded. E-mail containing PHI cannot be sent external to the ABPM e-mail server unless it is sent via the ABPM secure e-mail website.

Physical Safeguards

Once scanned, original documents are stored in a secure and locked area for at least six years and subsequently shredded or returned to the client customer, as appropriate. Discarded documents are stored in a secure location until shredded or returned.

Allegiance conducts periodic meetings with vendors to share privacy concerns, and to review vendor procedures and security issues. Contracted service providers and other entities with whom Allegiance must exchange confidential customer information are required to sign a Working Partner Agreement through which that entity agrees to maintain the confidentiality of customer information in accordance with Allegiance's privacy policies and applicable federal and state regulation.

GRAMM-LEACH-BLILEY ACT

IT IS THE OPINION OF INTERMOUNTAIN UNDERWRITERS, INC., AND ALLEGIANCE BENEFIT PLAN MANAGEMENT, INC., THAT THE GRAMM-LEACH-BLILEY ACT DOES NOT APPLY TO OUR COMPANIES; HOWEVER, THIS NOTICE IS TO ASSURE OUR CLIENT COMPANIES AND PLAN PARTICIPANTS OF THEIR MEDICAL AND FINANCIAL PRIVACY.

THE TYPE OF INFORMATION WE MAY COLLECT

We collect nonpublic personal information to support our normal business practices and to offer other benefit management services, as available. The type of information we collect and the extent to which it is used may vary depending on the products or services, and may include data such as addresses, telephone numbers, tax identification numbers, account information, employee information, employee health status and claim information, and other information related to the group health plan, benefits, and coverage. We obtain such information from the following sources: information we receive from individuals on applications or other forms they submit to us, information about transactions with us (including, for example, claims submissions), and information from our affiliates or others.

HOW INFORMATION IS PROTECTED

We restrict access to nonpublic personal information to those employees who need to know that information to provide products and services to our customers. We maintain physical, electronic, and procedural safeguards compliant with applicable federal and state regulations to protect the privacy of such information. All employees are required to maintain the confidentiality of nonpublic personal information and to follow our privacy policies.

When information is disclosed to entities, which perform services or functions on our behalf, we require them to adhere to policies and procedures to maintain the confidentiality of customer's nonpublic personal information, to use the information only for the limited purpose for which it was shared, and to abide by all applicable privacy regulations.

INFORMATION WE MAY DISCLOSE

In the course of conducting our business, we may disclose to third parties the information we collect about customers, as described above. These disclosures are only made as allowed by law, such as disclosures to affiliates, stop-loss carriers, and organizations that perform customer services or functions on our behalf, and to regulatory, law enforcement, and governmental authorities.

CATEGORIES OF INFORMATION WE DISCLOSE

We do not disclose any nonpublic personal information about our customers or former customers to anyone, except as permitted by law.

WHAT THE NEW PRIVACY REGULATIONS REQUIRE

Allegiance may provide individually-identifiable health information to treating health care providers for payment activities and healthcare operations and to Plan Administrators for plan administration functions. These activities and functions may include such as quality improvement activities, case management, care coordination, auditing, underwriting and premium rating activities, plan funding activities, such as stop-loss coverage and forecasting plan liability on high-dollar claims, customer service activities, determining eligibility or coverage limits, coordination of benefits, adjudication and subrogation of benefits, risk adjustment, billing, claims management, related data processing and claims review activities.

Valid authorization from the individual is required for Allegiance to use or disclose the individual's individually identifiable health information to a third party for purposes other than payment activities, healthcare operations, or plan administration functions.

DISCLOSURE OF INDIVIDUALLY-IDENTIFIABLE HEALTH INFORMATION

Unless Allegiance has valid authorization from the individual, specifically stating that his or her confidential health information may be discussed with specific individuals, such as the spouse, parent, employer or group plan representative, such information may only be disclosed to the individual or to the individual's treating health care providers. **In certain situations, mental health information may not be disclosed even to the individual without the consent of the treating provider**.

Even with valid authorization, Allegiance will only provide:

- The minimum necessary health information;
- To the specifically identified third party with need to know;
- For legitimate payment activities, healthcare operations or plan administration functions;
- In de-identified form, if possible.

BUSINESS AFFILIATES MUST AGREE TO MAINTAIN CONFIDENTIALITY

Covered entities, such as group health plans, are required to have written agreements with organizations with which the covered entity discloses individually-identifiable health information to protect the privacy and confidentiality of such information. These organizations must agree to maintain the privacy of any such information disclosed to them, in accordance with the terms of the agreement and applicable federal and state privacy regulations.

Allegiance, as an organization conducting activities on behalf of group health plans, and as a covered entity itself complies with all applicable federal and state regulations and laws.

APPENDIX B

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

Your Group Health Plan takes the privacy of your health information seriously. This Notice of Privacy Practices describes how protected health information (or "PHI") may be used or disclosed by your Group Health Plan to carry out payment, health care operations, and for other purposes that are permitted or required by law. This Notice of Privacy Practices also explains your Group Health Plan's legal obligations concerning your PHI, and describes your rights to access, amend and manage your PHI.

PHI is individually identifiable health information, including demographic information, collected from you or created and received by a health care provider, a health plan, your employer (when functioning on behalf of your group health plan), or a health care clearinghouse and that relates to: (i) your past, present or future physical or mental health or condition; (ii) the provision of health care to you; or (iii) the past, present, or future payment for the provision of health care to you.

This Notice of Privacy Practices has been drafted to be consistent with the HIPAA Privacy Rule. Any terms not defined in this Notice have the same meaning as they have in the HIPAA Privacy Rule. If you have any questions about this Notice or the policies and procedures described herein, you may contact the Allegiance Benefit Plan Management Privacy Official at 1-800-877-1122.

EFFECTIVE DATE

This Notice of Privacy Practices becomes effective on September 23, 2013.

THE PLAN'S RESPONSIBILITIES

Your Group Health Plan is required by law to maintain the privacy of your PHI. Your Group Health Plan is obligated to: provide you with a copy of a Notice of the Plan's legal duties and of its privacy practices related to your PHI; abide by the terms of the Notice that is currently in effect; and notify you in the event of a breach of your unsecured PHI. Your Group Health Plan reserves the right to change the provisions of its Notice and make the new provisions effective for all PHI that your Group Health Plan maintains. If your Group Health Plan makes a material change to its Notice, your Group Health Plan will make the revised Notice available to you by means of a legally compliant delivery method.

Permissible Uses and Disclosures of PHI

The following is a description of how your Group Health Plan is most likely to use and/or disclose your PHI.

Payment and Health Care Operations
Your Group Health Plan has the right to use and disclose your PHI for all activities that are included within the definitions of "payment" and "health care operations" as set out in 45 CFR § 164.501 (this provision is a part of the HIPAA Privacy Rule). Not all of the activities listed in this Notice are included within these definitions. Please refer to 45 CFR § 164.501 for a complete list. In order to administer your health benefits, your Group Health Plan may use or disclose your health information in various ways without your authorization, including:

- *Payment*
  Your Group Health Plan will use or disclose your PHI to pay claims for services provided to you and to obtain stop-loss reimbursements or to otherwise fulfill its responsibilities for coverage and providing benefits. For example, the Plan may disclose your PHI when a provider requests information regarding your eligibility for coverage under the Plan, or the Plan may use your information to determine if a treatment that you received was medically necessary.

- *Health Care Operations*

The Plan will use or disclose your PHI to support its business functions. These functions include, but are not limited to: quality assessment and improvement, reviewing provider performance, licensing, stop-loss underwriting, business planning, and business development. For example, the Plan may use or disclose your PHI: (i) to provide you with information about a disease management program; to respond to a customer service inquiry from you; or (ii) in connection with fraud and abuse detection and compliance programs. The PHI used or disclosed for these operational activities is limited to the minimum amount that is reasonably necessary to complete these tasks.

Other Permissible Uses and Disclosures of PHI

The following describes other possible ways in which the Plan may (and is permitted to) use and/or disclose your PHI.

- ***Required by Law***
  The Plan may use or disclose your PHI to the extent the law requires the use or disclosure. When used in this Notice, "required by law" is defined as it is in the HIPAA Privacy Rule. For example, the Plan may disclose your PHI when required by national security laws or public health disclosure laws.

- ***Public Health Activities***
  The Plan may use or disclose your PHI for public health activities that are permitted or required by law. For example, the Plan may use or disclose information for purpose of preventing or controlling disease, injury or disability, or the Plan may disclose such information to a public health authority authorized to receive reports of child abuse or neglect. The Plan also may disclose PHI, if directed by a public health authority, to a foreign government agency that is collaborating with the public health authority.

- ***Health Oversight Activities***
  The Plan may disclose your PHI to a health oversight agency for activities authorized by law, such as: audits: investigations; inspections; licensure or disciplinary actions; or civil, administrative, or criminal proceedings or actions. Oversight agencies seeking this information include government agencies that oversee: (i) the health care system; (ii) government benefit programs; other government regulatory programs; and (iv) compliance with civil rights laws.

- ***Abuse or Neglect***
  The Plan may disclose your PHI to a government authority that is authorized by law to receive reports of abuse, neglect or domestic violence. Additionally, as required by law, the Plan may disclose to a governmental entity authorized to receive such information, your PHI, if the Plan believes that you have been a victim of abuse, neglect, or domestic violence.

- ***Legal Proceedings***
  The Plan may disclose your PHI: (i) in the course of any judicial or administrative proceeding: (ii) in response to an order of a court or an administrative tribunal (to the extent such disclosure is expressly authorized); and (iii) in response to a subpoena, a discovery request, or other lawful process, once all administrative requirements of the HIPAA Privacy Rule have been met. For example, the Plan may disclose your PHI in response to a subpoena for such information but only after certain conditions of the HIPAA Privacy Rule are complied with.

- ***Law Enforcement***
  Under certain conditions, your Group Health Plan may also disclose your PHI to law enforcement officials. Some of the reasons for such a disclosure, for example, may include, but not be limited to: (i) it is required by law; (ii) it is necessary to locate or identify a suspect, fugitive, material witness, or missing person; and (iii) it is necessary to provide evidence of a crime that occurred on your Group Health Plan's premises.

- ***Coroners, Medical Examiners, Funeral Directors, Organ Donation Organizations***
  Your Group Health Plan may disclose PHI to a coroner or medical examiner for purposes of identifying a deceased person, determining a cause of death, or for the coroner or medical examiner to perform other duties authorized by law. Your Group Health Plan also may disclose, as authorized by law, information to funeral directors so that they may carry out their duties. Further, your Group Health Plan may disclose PHI to organizations that handle organ, eye, or tissue donation and transplantation.

- ***Research***
  Your Group Health Plan may disclose your PHI to researchers when an institutional review board or privacy board has: (i) reviewed the research proposal and established protocols to ensure the privacy of the information; and (ii) approved the research.

- ***To Prevent a Serious Threat to Health or Safety***
  Consistent with applicable federal and state laws, your Group Health Plan may disclose your PHI if your Group Health Plan believes that the disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public. Your Group Health Plan may also disclose PHI if it is necessary for law enforcement to identify or apprehend an individual.

- ***Military Activity and National Security, Protective Services***
  Under certain conditions, your Group Health Plan may disclose your PHI if you are, or were, Armed Forces personnel for activities deemed necessary by appropriate military command authorities. If you are a member of foreign military service, your Group Health Plan may disclose, in certain circumstances, your information to the foreign military authority.

- ***Inmates***
  If you are an inmate of a correctional institution, Your Group Health Plan may disclose your PHI to the correctional institution or to a law enforcement official for: (i) the institution to provide health care to you; (ii) your health and safety and the health and safety of others; or (iii) the safety and security of the correctional institution.

- ***Workers' Compensation***
  Your Group Health Plan may disclose your PHI to comply with workers' compensation laws and other similar programs that provide benefits for work-related injuries or illnesses.

- ***Emergency Situations***
  Your Group Health Plan may disclose your PHI in an emergency situation, or if you are incapacitated or not present, to a family member, close personal friend, authorized disaster relief agency, or any other person previously identified by you. Your Group Health Plan will use professional judgment and experience to determine if the disclosure is in your best interests. If the disclosure is in your best interest, your Group Health Plan will disclose only the PHI that is directly relevant to the person's involvement in your case.

- ***Fundraising Activities***
  Your Group Health Plan may use or disclose your PHI for fundraising activities, such as raising money for a charitable foundation or similar entity to help finance its activities. If your Group Health Plan contacts you for fundraising activities, your Group Health Plan will give you the opportunity to opt-out or stop receiving such communications in the future.

- ***Group Health Plan Disclosures***
  Your Group Health Plan may disclose your PHI to a sponsor of the group health plan – such as an employer or other entity – that is providing a health care program to you. Your Group Health Plan can disclose your PHI to that entity if that entity has contracted with us to administer your health care program on its behalf.

- ***Underwriting Purposes***
  Your Group Health Plan may use or disclose your PHI for underwriting purposes, such as to make a determination about a coverage application or request. If your Group Health Plan does use or disclose your PHI for underwriting purposes, your Group Health Plan is prohibited from using or disclosing in the underwriting process your PHI that is genetic information.

- ***Others Involved in Your Health Care***
  Using its best judgment, your Group Health Plan may make your PHI known to a family member, other relative, close personal friend or other personal representative that you identify. Such a use will be based on how involved the person is in your care, or payment that relates to your care. Your Group Health Plan may release information to parents or guardians if allowed by law.

If you are not present or able to agree to these disclosures of your PHI Your Group Health Plan, using its professional judgment, may determine whether the disclosure is in your best interest.

Uses and Disclosures of Your PHI that Require Your Authorization

Sale of PHI
Your Group Health Plan will request your written authorization before it makes any disclosure that is deemed a sale of your PHI, meaning that Your Group Health Plan is receiving compensation for disclosing the PHI in this manner.

Marketing
Your Group Health Plan will request your written authorization to use or disclose your PHI for marketing purposes with limited exceptions, such as when the Plan has face-to–face marketing communications with you or when your Group Health Plan provides promotional gifts of nominal value.

Psychotherapy Notes
Your Group Health Plan will request your written authorization to use or disclose any of your psychotherapy notes that the Plan may have on file with limited exception, such as for certain treatment, payment or health care operation functions.

Other uses and disclosures of your PHI that are not described above will be made only with your written authorization. If you provide Your Group Health Plan with such an authorization, you may revoke the authorization in writing and this revocation will be effective for future uses and disclosures of PHI. However, the revocation will not be effective for information Your Group Health Plan has already used or disclosed, relying on the authorization.

Required Disclosures of Your PHI

The following describes disclosures that your Group Health Plan is required by law to make.

- ***Disclosures to the Secretary of the U.S. Department of Health and Human Services***
  Your Group Health Plan is required to disclose your PHI to the Secretary of the U.S. Department of Health and Human Services when the Secretary is investigating or determining the Plan's compliance with the HIPAA Privacy Rule.

- ***Disclosures to You***
  Your Group Health Plan is required to disclose to you most of your PHI in a "designated record set" when you request access to this information. Generally, a "designated record set" contains medical and billing records as well as other records that are used to make decisions about your health care benefits. Your Group Health Plan also is required to provide, upon your request, an accounting of most disclosures of your PHI that are for reasons other than payment and health care operations and are not disclosed through a signed authorization.

  Your Group Health Plan will disclose your PHI to an individual who has been designated by you as your personal representative and who has qualified for such designation in accordance with applicable state law. However, before Your Group Health Plan will disclose PHI to such a person, you must submit a written notice of his/her designation, along with the documentation that supports his/her qualification (such as a power of attorney).

Even if you designate a personal representative, the HIPAA Privacy Rule permits your Group Health Plan to elect not to treat the person as your personal representative if the Plan has a reasonable belief that: (i) you have been, or may be, subjected to domestic violence, abuse or neglect by such person; (ii) treating such person as your personal representative could endanger you; or (iii) your Group Health Plan determines, in the exercise of its professional judgment, that it is not in your best interest to treat the person as your personal representative.

- ***Business Associates***
  Your Group Health Plan contracts with individuals and entities (Business Associates) to perform various functions on its behalf or to provide certain types of services. To perform these functions or to provide the services, the Business Associates will receive, create, maintain, use or disclose PHI, but only after the Business Associate agrees in writing to contract terms designed to appropriately safeguard your information. For example, the Plan may disclose your PHI to a Business Associate to administer claims or to provide member service support, utilization management,

subrogation, or pharmacy benefit management.

- ***Other Covered Entities***
  Your Group Health Plan may use or disclose your PHI to assist health care providers in connection with their treatment or payment activities, or to assist other covered entities in connection with payment activities and certain health care operations. For example, your Group Health Plan may disclose your PHI to a health care provider when needed by the provider to render treatment to you, and it may disclose PHI to another covered entity to conduct health care operations in the areas of quality assurance and improvement activities, or accreditation, certification, licensing or credentialing. This also means that your Group Health Plan may disclose or share your PHI with insurance carriers in order to coordinate benefits if you or your family members have coverage through another carrier.

- ***Plan Sponsor***
  Your Group Health Plan may disclose your PHI to the plan sponsor of your Group Health Plan for purposes of plan administration or pursuant to an authorization request signed by you.

Potential Impact of State Law

The HIPAA Privacy Rule regulations generally do not "preempt" (or take precedence over) state privacy or other applicable laws that provide individuals greater privacy protections. As a result, to the extent state law applies, the privacy laws of a particular state, or other federal laws, rather than the HIPAA Privacy Rule regulations, might impose a privacy standard under which your Group Health Plan will be required to operate. For example, where such laws have been enacted, the Plan will follow more stringent state privacy laws that relate to uses and disclosures of PHI concerning HIV or AIDS, mental health, substance abuse/chemical dependency, genetic testing, reproductive rights, etc.

YOUR RIGHTS

- **Right to Request Restrictions**
  You have the right to request a restriction on the PHI your Group Health Plan uses or discloses about you for payment or health care operations. Your Group Health Plan is *not* required to agree to any restriction that you may request. If your Group Health Plan does agree to the restriction, it will comply with the restriction unless the information is needed to provide you with emergency treatment. You may request a restriction by contacting the designated contact of your Group Health Plan. It is important that you direct your request for restriction to the designated contact to initiate processing your request. Requests sent to persons or offices other than the designated contact could delay processing the request.

  Your Group Health Plan needs to receive this information in writing and will instruct you where to send your request when you call. In your request please provide: (1) the information whose disclosure you want to limit; and (2) how you want to limit the use and/or disclosure of the information.

- ***Right to Request Confidential Communications***
  If you believe that a disclosure of all or part of your PHI may endanger you, you may request that the Plan communicate with you regarding your information in an alternative form or at an alternative location. For example, you may ask that the Plan only contact you at your work address or through your work e-mail.

  You may request a restriction by contacting the designated contact the designated contact of your Group Health Plan. It is important that you direct you request for confidential communications to the designated contact so that your Group Health Plan can begin to process your request. Requests sent to persons or offices other than your Group Health Plan's designated contact might delay processing the request.

  Your Group Health Plan needs to receive this information in writing and will instruct you where to send your request when you call. In your request please explain: (1) that you want your Group Health Plan to communicate your PHI with you in an alternative manner or at an alternative location; and (2) that the disclosure of all or part of the PHI in a manner inconsistent with your instructions would put you in danger.

  Your Group Health Plan will accommodate a request for confidential communications that is reasonable and that states that the disclosure of all or part of your PHI could endanger you. As permitted by the HIPAA Privacy Rule,

"reasonableness" will include, when appropriate, making alternate arrangements regarding payment.

Accordingly, as a condition of granting your request, you will be required to provide your Group Health Plan information concerning how payment will be handled. For example, if you submit a claim for payment, state or federal law (or your Group Health Plan's own contractual obligations) may require that your Group Health Plan disclose certain financial claim information to the plan participant (e.g., an Explanation of Benefits or "EOB"). Unless you have made other payment arrangements, the EOB (in which your PHI might be included) may be released to the plan participant.

Once your Group Health Plan receives all of the information for such a request (along with instructions for handling future communications) the request will be processed as soon as practicable. Prior to receiving the information necessary for this request, or during the time it takes to process it, PHI might be disclosed (such as through an EOB). Therefore, it is extremely important that you contact the designated contact for your Group Health Plan as soon as you determine that you need to restrict disclosures of your PHI.

If you terminate your request for confidential communications, the restriction will be removed for all of your PHI your Group Health Plan holds including PHI that was previously protected. Therefore, you should not terminate a request for confidential communications if you remain concerned that disclosure of your PHI will endanger you.

- ***Right to Inspect and Copy***

You have the right to inspect and copy your PHI that is contained in a "designated record set." Generally, a designated record set contains medical and billing records as well as other records that are used to make decisions about your health care benefits. However, you may not inspect or copy psychotherapy notes or certain other information that may be contained in a designated record set.

To inspect and copy your PHI that is contained in a designated record set, you must submit your request to your Group Health Plan's designated contact. It is important that you contact the designated contact to request an inspection and copying so that your Group Health Plan can begin to process your request. Requests sent to persons, offices, other than the designated contact might delay processing the request. If you request a copy of the information, your Group Health Plan may charge a fee for the costs of copying, mailing, or other supplies associated with your request. The requested information will be provided within thirty (30) days if the information is maintained on site or within sixty (60) days if the information is maintained offsite. A single thirty (30) day extension is allowed if your Group Health Plan is unable to comply with this deadline.

The Plan may deny your request to inspect and copy in certain limited circumstances. If you are denied access to your information, you may request that the denial be reviewed. To request a review, you must contact your Group Health Plan's designated contact. A licensed health care professional chosen by us will review your request and the denial. The person performing this review will not be the same one who denied your initial request. Under certain conditions, the denial will not be reviewable. If this event occurs, your Group Health Plan will inform you of this fact.

- ***Right to Amend***

If you believe the PHI The Plan has for you is inaccurate or incomplete, you may request that it be amended. You may request that to your Group Health Plan amend your information by contacting your Group Health Plan's designated contact. Additionally, your request should include the reason the amendment is necessary. It is important that you direct your request for amendment to the designated contact to initiate processing your request. Requests sent to persons or offices, other than the designated contact, might delay processing the request. Your Group Health Plan will have sixty (60) days after the request is made to act on the request. A single thirty (30) day extension is allowed if your Group Health Plan is unable to comply with this deadline.

In certain cases, your Group Health Plan may deny your request for an amendment. For example, your Group Health Plan may deny your request if the information you want to amend is not maintained by your Group Health Plan, but by another entity or if your Group Health Plan determines that your information is accurate and complete. If your Group Health Plan denies your request you have the right to file a statement of disagreement with your Group Health Plan. Your statement of disagreement will be linked with the disputed information and all future disclosures of the disputed information will include your statement.

- ***Right to Accounting***

You have a right to an accounting of certain disclosures of your PHI that are for reasons other than treatment, payment or health care operations. No accounting of disclosures is required for disclosures made pursuant to a signed authorization by you or your personal representative. You should know that most disclosures of PHI will be for purposes of payment or health care operations, and, therefore, will not be subject to your right to an accounting. There also are other exceptions to this right.

An accounting will include the dates of the disclosure, to whom the disclosure was made, a brief description of the information disclosed, and the purpose for the disclosure.

You may request an accounting by submitting your request in writing to your Group Health Plan's designated contact. It is important that you direct your request for an accounting to the designated contact so that your Group Health Plan can begin to process the request. Requests sent to persons or offices other than the designated contact might delay processing the request. If the accounting cannot be provided within sixty (60) days, an additional thirty (30) days is allowed if a written statement explaining the reasons for the delay is provided. Your request may be for disclosures made up to six (6) years before the date of your request but not for disclosures made before April 14, 2003. If you request more than one accounting within a twelve (12) month period, your Group Health Plan may charge you the reasonable costs of providing the accounting. Your Group Health Plan will notify you of the cost involved and you may choose to withdraw or modify your request before any costs are incurred.

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

You have the right to request a copy of this Notice at any time by contacting your Group Health Plan's designated contact. If you receive this Notice on the Plan's Website or by electronic mail, you are entitled to request a paper copy of this Notice.

CHANGES TO THIS NOTICE

Your Group Health Plan reserves the right to change its Notice and make any revised Notice effective for health information already on file for you, as well as any health information your Group Health Plan receives in the future. The most recent Notice will be posted in a prominent location to which you have access.

COMPLAINTS

You may complain to your Group Health Plan if you believe it has violated your privacy rights. You may file a complaint with your Group Health Plan by contacting your Group Health Plan's designated contact.

You may also file a complaint with the Secretary of the U.S. Department of Health and Human Services. Complaints filed directly with the Secretary must: (1) be in writing; (2) contain the name of the entity you are complaining about; (3) describe the relevant problems; and (4) be filed within 180 days of the time you became or should have become aware of the problem.

Your Group Health Plan will not penalize or retaliate against you in any way for filing a complaint.

APPENDIX C

Note: A separate form must be completed for each person age eighteen or older.

AUTHORIZATION TO RELEASE CONFIDENTIAL HEALTH AND CLAIM INFORMATION

_____ has requested health and/or claims information concerning claims submitted and paid for the covered person(s) shown below. Because laws exist to protect the privacy of confidential health and claims information, we need valid authorization from you, the Covered Person, to disclose this information to the requesting party. Please sign the following form in the presence of a Notary Public and return the completed form to Allegiance Benefit Plan Management, Inc., P.O. Box 3018, Missoula, MT 59806.

Name of Employer Plan: _____

Group Number: _____

Name of Covered Person: _____

Social Security Number of Covered Person: _____

Name of Dependent(s)/Birth Date _____

_____

_____

As the Covered Person under the above-named group health plan, I hereby authorize Allegiance Benefit Plan Management, Inc. to release the following confidential health and claims related information:

_____

_____

_____

This information may be disclosed to: _____, at the following address,

_____, whose relationship to the Covered Person is:

_____, for the following purpose(s):

- _____ To determine eligibility for benefits, enrollment in a group health plan, or for underwriting determinations;
- _____ For payment of provider claims;
- _____ Other: _____

I agree to indemnify and hold the Plan Supervisor harmless for confidential health and/or claims information released to the named person(s) based upon this authorization.

This authorization will remain valid until the Covered Person is no longer covered under the above-named group health plan, for two years, or until the following date: _____, whichever occurs earlier.

I understand I may revoke this authorization at any time, upon written notice to Allegiance Benefit Plan Management, Inc., P.O. Box 3018, Missoula, MT 59806, unless either: 1) Allegiance has already disclosed my confidential information in reliance upon this authorization; or 2) this authorization was a condition of my enrollment in the group health plan.

I understand that Allegiance may not condition treatment, payment of claims, enrollment in a group health plan or eligibility for benefits upon this authorization, UNLESS this authorization is expressly for the purposes of determining eligibility for benefits, enrollment, or for underwriting or risk rating determinations.

I understand that any confidential health and/or claims information disclosed to the requesting party in accordance with this Authorization may be re-disclosed by the requesting party and at that point, would no longer be protected by this Authorization.

_____ _____

Signature of Covered Person Date

STATE OF _____

COUNTY OF _____

Signed and acknowledged by _____ who provided proof of identification and who personally appeared before me, a Notary Public, this ____ day of _____, 20___.

_____

(Seal) Signature of Notary Public

My commission expires _____.

APPENDIX D

PLAN DOCUMENT AMENDMENT

HIPAA PRIVACY AND SECURITY STANDARDS

These standards are intended to comply with all requirements of the Privacy and Security Rules of the Administrative Simplification Rules of HIPAA as stated in 45 CFR Parts 160, 162 and 164, as amended from time to time.

DEFINITIONS

"Protected Health Information" (PHI) means information, including demographic information, that identifies an individual and is created or received by a health care provider, health plan, employer, or health care clearinghouse; and relates to the physical or mental health of an individual; health care that individual has received; or the payment for health care provided to that individual. PHI does not include employment records held by the Plan Sponsor in its role as an employer.

"Summary Health Information" means information summarizing claims history, expenses, or types of claims by individuals enrolled in a group health plan and has had the following identifiers removed: names; addresses, except for the first three digits of the zipcode; dates related to the individual (ex: birth date); phone numbers; email addresses and related identifiers; social security numbers; medical record numbers; account or plan participant numbers; vehicle identifiers; and any photo or biometric identifier.

PRIVACY CERTIFICATION

The Plan Sponsor hereby certifies that the Plan Documents have been amended to comply with the privacy regulations by incorporation of the following provisions. The Plan Sponsor agrees to:

1. Not use or further disclose the information other than as permitted or required by the Plan Documents or as required by law. Such uses or disclosures may be for the purposes of plan administration, including but not limited to, the following:

    A. Operational activities such as quality assurance and utilization management, credentialing, and certification or licensing activities; underwriting, premium rating or other activities related to creating, renewing or replacing health benefit contracts (including reinsurance or stop loss); compliance programs; business planning; responding to appeals, external reviews, arranging for medical reviews and auditing, and customer service activities. Plan administration can include management of carve-out plans, such as dental or vision coverage.

    B. Payment activities such as determining eligibility or coverage, coordination of benefits, determination of cost-sharing amounts, adjudicating or subrogating claims, claims management and collection activities, obtaining payment under a contract for reinsurance or stop-loss coverage, and related data-processing activities; reviewing health care services for medical necessity, coverage or appropriateness of care, or justification of charges; or utilization review activities.

C. For purposes of this certification, plan administration does not include disclosing Summary Health Information to help the plan sponsor obtain premium bids; or to modify, amend or terminate group health plan coverage. Plan administration does not include disclosure of information to the Plan Sponsor as to whether the individual is a participant in; is an enrollee of or has disenrolled from the group health plan.

2. Ensure that any agents, including a subcontractor, to whom it provides PHI received from the Plan agree to the same restrictions and conditions that apply to the Plan Sponsor with respect to such information;

3. Not use or disclose the PHI for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the Plan Sponsor;

4. Report to the Plan any use or disclosure of the information that is inconsistent with the uses or disclosures provided for of which it becomes aware;

5. Make available PHI as required to allow the Covered Person a right of access to his or her PHI as required and permitted by the regulations;

6. Make available PHI for amendment and incorporate any amendments into PHI as required and permitted by the regulations;

7. Make available the PHI required to provide an accounting of disclosures as required by the regulations;

8. Make its internal practices, books, and records relating to the use and disclosure of PHI received from the Plan available to any applicable regulatory authority for purposes of determining the Plan's compliance with the law's requirements;

9. If feasible, return or destroy all PHI received from the Plan that the Plan Sponsor still maintains in any form and retain no copies of such information when no longer needed for the purpose for which disclosure was made, except that, if such return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible; and

10. Ensure that the adequate separation required between the Plan and the Plan Sponsor is established. To fulfill this requirement, the Plan Sponsor will restrict access to nonpublic personal information to the Plan Administrator(s) designated in this Plan Document or employees designated by the Plan Administrator(s) who need to know that information to perform plan administration and healthcare operations functions or assist eligible persons enrolling and disenrolling from the Plan. The Plan Sponsor will maintain physical, electronic, and procedural safeguards that comply with applicable federal and state regulations to guard such information and to provide the minimum PHI necessary for performance of healthcare operations duties. The Plan Administrator(s) and any employee so designated will be required to maintain the confidentiality of nonpublic personal information and to follow policies the Plan Sponsor establishes to secure such information.

When information is disclosed to entities that perform services or functions on the Plan's behalf, such

entities are required to adhere to procedures and practices that maintain the confidentiality of the Covered Person's nonpublic personal information, to use the information only for the limited purpose for which it was shared, and to abide by all applicable privacy laws.

SECURITY CERTIFICATION

The Plan Sponsor hereby certifies that its Plan Documents have been amended to comply with the security regulations by incorporation of the following provisions. The Plan Sponsor agrees to:

1. Implement and follow all administrative, physical, and technical safeguards of the HIPAA Security Rules, as required by 45 CFR §§164.308, 310 and 312.

2. Implement and install adequate electronic firewalls and other electronic and physical safeguards and security measures to ensure that electronic PHI is used and disclosed only as stated in the Privacy Certification section above.

3. Ensure that when any electronic PHI is disclosed to any entity that performs services or functions on the Plan's behalf, that any such entity shall be required to adhere to and follow all of the requirements for security of electronic PHI found in 45 CFR §§164.308, 310, 312, 314 and 316.

4. Report to the Plan Administrator or the Named Fiduciary of the Plan any attempted breach, or breach of security measures described in this certification, and any disclosure or attempted disclosure of electronic PHI of which the Plan Sponsor becomes aware.

APPENDIX D

PRIVACY AND CONFIDENTIALITY NOTICE

Allegiance Benefit Plan Management, Inc. is providing the following claims records ("Claims Information") on behalf of a group health plan and/or flexible benefits plan. The Claims Information is being provided for the limited purpose of claims payment, coordination of benefits, or related plan administration functions. The Claims Information may contain medical and other information protected as confidential and private by the Privacy Act of 1974, as amended, the privacy regulations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended, and other applicable state and federal regulations.

The Health Insurance Portability and Accountability Act of 1996 specifically states that individually-identifiable health information may be provided without a valid authorization from the claimant for limited reasons – claims payment, coordination of benefits, or related plan administration functions. Allegiance will not provide individually-identifiable health information for any other purpose without the individual's valid authorization.

It may be a violation of federal and state laws to disclose the Claims Information, or any portion of it, in any manner that is likely to, or that does in fact, reveal the identity of any person named in the Claims Information to any person or entity, except those individuals who are expressly authorized to view it for legitimate purposes. It may also be a violation of ERISA or other applicable laws to use this information in any manner that could result in the person who is the subject of the information from being denied any employment opportunities or having employment terminated.

The person receiving this information is, personally and on behalf of the group health plan or flexible benefits plan, hereby put on notice that the following information is, or may be, confidential in nature and should not be disclosed in any manner, to any person or entity, except as is inherently and necessarily required for claims payment, coordination of benefits, or other plan administration functions. The person receiving this information is responsible to protect the confidentiality of anyone who may be identified, or could reasonably be identified, from the protected health information being provided. Further, any person receiving this information who believes he or she cannot abide by the terms of this notice should immediately return any and all information being provided with this notice to Allegiance Benefit Plan Management, Inc., who is acting on behalf of the group health plan or flexible benefits plan.