



**SPECIAL DISTRICTS INSURANCE SERVICES
EMPLOYEE BENEFIT PLAN**

HIPAA HEALTH INFORMATION PRIVACY POLICIES

**SPECIAL DISTRICTS INSURANCE SERVICES
EMPLOYEE BENEFIT PLAN**

HIPAA HEALTH INFORMATION PRIVACY POLICIES

Table of Contents

	Page
Preamble	1
Article 1 General.....	2
1.1 Purpose.....	2
1.2 Scope of Privacy Policies.....	2
1.3 No Third Party Rights.....	2
1.4 Hybrid Plan Safeguards	2
1.5 Amendment.....	2
1.6 Effective Date	2
Article 2 Definitions	3
Article 3 Administrative Policies.....	9
3.1 Privacy Official and Contact Person.....	9
3.2 Training.....	9
3.3 Technical and Physical Safeguards.....	9
3.4 Notice of Privacy Practices	10
3.5 Complaint Process	11
3.6 Sanctions for Violations of Privacy Policy	12
3.7 Mitigation of Inadvertent Disclosures	12
3.8 No Intimidating or Retaliatory Acts	12
3.9 Plan Document Standard.....	13
3.10 Documentation Standard.....	14
Article 4 Use and Disclosure of Protected Health Information	16
4.1 General.....	16
4.2 Prohibited Uses and Disclosures.....	16
4.3 Payment or Operations Purposes	16
4.4 Authorization for Release of PHI	17
4.5 Disclosures to Involved Persons	18
4.6 De-Identified Information	19
4.7 Other Sanctioned Disclosures	20
4.8 “Minimum Necessary” Standard	21
4.9 Disclosures Regarding Minors, Dependents and Descendants.....	22
4.10 Verification of Identity and Authority	23
Article 5 Requests for Privacy Protections	25
5.1 Requested Restriction of Uses and Disclosures.....	25
5.2 Request for Confidential Communications.....	26
Article 6 Right of Access to Protected Health Information.....	27
6.1 General Right of Access	27
6.2 Non-Appealable Denials of Access	27
6.3 Reviewable Denials of Access.....	27

6.4	Responding to Request	28
6.5	Form of Access	28
6.6	Fees	28
6.7	Access Denial Procedures	29
6.8	Redirection of Requests	29
6.9	Documentation	29
Article 7	Amendment of Protected Health Information	30
7.1	Right to Amend	30
7.2	Grounds for Denial	30
7.3	Timing of Action	30
7.4	Effecting the Amendment	30
7.5	Denial of Amendment Request	31
7.6	Statement of Disagreement	31
7.7	Notation of Disagreement	32
7.8	Effect of Denial on Subsequent Disclosures	32
7.9	External Notice of Amendment	32
7.10	Documentation	32
Article 8	Accounting of Disclosures of Protected Health Information	33
8.1	Right to an Accounting	33
8.2	Accountable Disclosures	33
8.3	Ineligible Disclosures	33
8.4	Temporary Suspension of Accountings	34
8.5	Content of the Accounting	34
8.6	Deadline for Providing Accounting	35
8.7	Documentation	35
Article 9	Disclosures to Business Associates	37
9.1	Restrictions on Disclosures	37
9.2	Business Associates	37
9.3	Managing Business Associate Contracts	38
9.4	Plan Responsibilities	38
9.5	Business Associate's Responsibilities	38
9.6	Unauthorized Use or Disclosure	39
9.7	No Liability for the Actions of Business Associates	39
Article 10	Notification in the Case of Breach	40
10.1	General	40
10.2	Definitions	40
10.3	Presumption of Breach	41
10.4	Notice to Covered Individuals	41
10.5	Content of Notification	42
10.6	Notice to Media Outlets	42
10.7	Notice to HHS	42
10.8	Timeliness of Notification	42
10.9	Breaches Treated as Discovered	42
10.10	Business Associates	43
10.11	Delay of Notification Authorized for Law Enforcement Purposes	43

**SPECIAL DISTRICTS INSURANCE SERVICES
EMPLOYEE BENEFIT PLAN**

HIPAA HEALTH INFORMATION PRIVACY POLICIES


Preamble

WHEREAS, the Special Districts Insurance Services Employee Benefit Plan (the “Plan”) is maintained for the benefit of eligible active and former employees; and

WHEREAS, the Plan has designated a Privacy Official to develop and implement policies with respect to protected health information maintained under the Plan, (the “Privacy Policies”), which Privacy Policies are designed to comply with the HIPAA Privacy Rule standards prescribed by federal regulations issued by the U.S. Department of Health and Human Services.

NOW, THEREFORE, in consideration of the foregoing, the Privacy Official hereby adopts the Privacy Policies prescribed herein, effective generally as of July 1, 2022.

SPECIAL DISTRICTS INSURANCE SERVICES
EMPLOYEE BENEFIT PLAN

By: 
Frank Stratton, Privacy Official

Dated: July 1st, 2024

PDX\126319\191678\WWM\16089332.1

ARTICLE 1

General

1.1 Purpose. The Special Districts Insurance Services Employee Benefit Plan (the “Plan”) is maintained for the benefit of its eligible active and former employees and their dependents. The Special Districts Insurance Services Trust (“SDIS”) serves as the Plan Administrator. Certain members of the SDIS workforce have the need for access to health information of persons covered under the Plan in order to carry out their duties with respect to the Plan. The Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) and its implementing regulations restrict use and disclosure of health information so as to preserve its privacy. Toward that end, the use and disclosure of health information under the Plan will be governed by these Privacy Policies.

1.2 Scope of Privacy Policies. To the extent these Privacy Policies establish requirements and obligations above and beyond those required by HIPAA, the Privacy Policies will not be binding upon SDIS. These Privacy Policies do not address any obligations prescribed under other federal or state laws.

1.3 No Third Party Rights. No third party rights (including, but not limited to, rights of Covered Individuals and their beneficiaries, or of any Business Associates) are intended to be created by these Privacy Policies.

1.4 Hybrid Plan Safeguards. The Plan is a hybrid plan consisting of Health Care Components and benefit programs that are not Health Care Components. The benefit programs that are not Health Care Components are not subject to these Privacy Policies. Nevertheless, in order to ensure that the Health Care Components of the Plan comply with the HIPAA Privacy Rule, the safeguard provisions described below shall be applicable.

(a) PHI arising under a Health Care Component shall not be disclosed in connection with a non-Health Care Component of the Plan in circumstances in which such disclosure would be prohibited if the Health Care Component and other component were maintained under separate plans.

(b) If a Workforce Member performs duties for a designated Health Care Component and for another component of the Plan in the same capacity, the Workforce Member must not use or disclose PHI created or received in the course of or incident to the Workforce Member’s work for the Health Care Component in a manner prohibited by the HIPAA Privacy Rule.

1.5 Amendment. Notwithstanding any provision of these Privacy Policies to the contrary, the Privacy Official may, at any time or from time to time, amend these Privacy Policies in whole or in part. Any amendment of these Privacy Policies will be effectuated by a written instrument signed by the Privacy Official.

1.6 Effective Date. The provisions of these Privacy Policies as herein amended and restated will be effective as of June 1, 2015, except as may be specifically provided otherwise.

ARTICLE 2

Definitions

When used in these Privacy Policies, certain terms have the respective meanings set forth in this Article, or in certain other Articles of these Policies.

Business Associate. “Business Associate” means an organization or a person (other than a Workforce Member) who on behalf of the Plan performs or assists in the performance of a function or activity involving the use or disclosure of a Covered Individual’s PHI, as more fully defined in Section 9.2.

Covered Individual. “Covered Individual” means a person who is covered under the Plan and who is the subject of the PHI at issue. The term also includes someone who qualifies as a personal representative of such an individual.

Disclosure. “Disclosure” means, in regard to any PHI, any release, transfer, provision of access to, or divulging in any other manner of individually identifiable health information to a person who is not a Workforce Member.

Family Member.

(a) “Family Member” means, with respect to a Covered Individual:

(i) A dependent of such Covered Individual (as defined in paragraph (b)(i) below); or

(ii) Any other individual with respect to the Covered Individual or of a dependent of the Covered Individual who is a first-degree, second-degree, third-degree or fourth-degree relative as defined in subsection (b) below.

(b) For purposes of establishing an individual’s status as a Family Member, the rules below will apply.

(i) A “dependent” means any individual who is or may become eligible for coverage under a Health Care Component of the Plan.

(ii) First-degree relatives include a Covered Individual’s parents, spouses, siblings and children.

(iii) Second-degree relatives include a Covered Individual’s grandparents, grandchildren, uncles, aunts, nephews, and nieces.

(iv) Third-degree relatives include a Covered Individual’s great-grandparents, great grandchildren, great uncles and aunts, and first cousins.

(v) Fourth-degree relatives include a Covered Individual’s great-great grandparents, great-great grandchildren, and children of the first cousins.

(vi) Relatives by affinity (such as by marriage or adoption) will be treated the same as relatives by consanguinity (i.e., relatives who share a common biological ancestor).

(vii) Relatives by less than full consanguinity (i.e., half-siblings, who share only one parent) will be treated the same as relatives by full consanguinity (such as siblings who share both parents).

Genetic Information.

(a) “Genetic Information” with respect to a Covered Individual means information concerning:

(i) Genetic Tests of the Covered Individual or of the Covered Individual’s Family Members;

(ii) The manifestation of a disease or disorder in a Family Member of the Covered Individual (i.e., family medical history);

(iii) A request for, or receipt of, Genetic Services by the Covered Individual or Family Member; or

(iv) The Covered Individual’s participation in clinical research that includes Genetic Services.

(b) Genetic Information also constitutes information relating to:

(i) A fetus carried by a Covered Individual, or by a Family Member of such an individual; or

(ii) Any embryo legally held by the Covered Individual, or by a Family Member of such an individual using an assisted reproductive technology.

(c) The term “Genetic Information” does not include information about the sex or age of any Covered Individual or Family Member.

Genetic Services. “Genetic Services” means:

(a) A Genetic Test;

(b) Genetic counseling (including obtaining, interpreting, or assessing Genetic Information); or

(c) Genetic education.

Genetic Test.

(a) In general, the term “Genetic Test” means an analysis of human DNA, RNA, chromosomes, proteins, or metabolites that detects genotypes, mutations, or chromosomal changes.

(b) A Genetic Test does not include an analysis of proteins or metabolites that is directly related to a manifested disease, disorder, or pathological condition.

Health Care Components. “Health Care Components” mean a benefit program maintained as part of the Plan that provides medical care to employees or their dependents, either directly or through insurance.

Health Care Operations. “Health Care Operations” means any of the following activities performed by or on behalf of the Plan:

(a) Quality assessment and improvement activities, population based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives, or related functions that do not include treatment;

(b) Reviewing the competence or qualifications of health care professionals, and evaluating practitioner, provider or health plan performance;

(c) Enrollment, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance);

(d) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;

(e) Business planning and development, such as conducting cost management and planning related analyses related to managing and operating the Plan, including formulary development and administration, development or improvement of methods of payment or coverage policies; and

(f) Business management and general administrative activities of the Plan, including, but not limited to, activities relating to the implementation of and compliance with the HIPAA Privacy Rule, resolution of claims and internal grievances, and creating “de-identified health information” described in Section 4.6.

HHS. The “HHS” means the U.S. Department of Health and Human Services.

HIPAA. “HIPAA” means the Health Insurance Portability and Accountability Act of 1996.

HIPAA Privacy Rule. “HIPAA Privacy Rule” means the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, Subparts A and E.

Individual Identifiable Health Information. For purposes of these Privacy Policies, “Individual Identifiable Health Information” means information with respect to any Covered Individual that is a subset of health information, including demographic information collected from a covered individual, that:

- (a) Is created or received by the Plan;
- (b) Relates to the past, present, or future physical or mental health or condition of the Covered Individual, the provision of health care to the Covered Individual, or the past, present or future payment for the provision of health care to the Covered Individual; and
- (c) Identifies the Covered Individual, or for which there is a reasonable basis to believe the information can be used to identify the Covered Individual.

Manifested. A disease, disorder, or pathological condition of a Covered Individual is considered to have been “Manifested” if the Covered Individual has been or could reasonably be diagnosed with the disease, disorder, or pathological condition by a health care professional with appropriate training and expertise in the field of medicine involved. A disease, disorder, or pathological condition of a Covered Individual is not manifested if the diagnosis is based principally on Genetic Information.

Payment. Except as prohibited under Section 4.2, “Payment” means the activities undertaken by SDIS on behalf of the Plan to obtain premiums, to determine or fulfill the Plan’s responsibility for coverage and provision of benefits, or to obtain or provide reimbursement for the provision of health care. Such activities may include, but are not limited to, the following:

- (a) Determinations of eligibility or coverage (including the coordination of benefits or the determination of cost sharing amounts), and the adjudication or subrogation of health benefit claims;
- (b) Risk adjusting amounts that are due based on enrollee health status and demographic characteristics;
- (c) Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop loss insurance and excess of loss insurance), and related health care data processing;
- (d) Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;
- (e) Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and

(f) Disclosures to a consumer reporting agency of any of the following components of PHI relating to collection of premiums or reimbursement of benefit payments: name and address, date of birth, social security number, payment history, account number and name and address of the Plan.

Plan. “Plan” means the Special Districts Insurance Services Employee Benefit Plan.

Privacy Policies. “Privacy Policies” means the health information privacy policies and procedures applicable to the Plan, as set forth in this document.

Protected Health Information.

(a) For purposes of these Privacy Policies, “Protected Health Information” means Individually Identifiable Health Information that is:

- (i) Transmitted by electronic media;
- (ii) Maintained in electronic media; or
- (iii) Transmitted or maintained in any other form or medium.

(b) Protected Health Information excludes Individually Identifiable Health Information:

- (i) In employment records held by SDIS in its role as employer; and
- (ii) Regarding a person who has been deceased for more than 50 years.

SDIS. “SDIS” means the Special Districts Insurance Services Trust.

Underwriting Purposes. “Underwriting Purposes” means with respect to the Plan, or health insurance coverage offered in connection with the Plan:

(a) Rules for, or determination of, eligibility (including enrollment and continued eligibility) for benefits under the Plan (including changes in deductibles or other cost-sharing mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program);

(b) The computation of premium or contribution amounts under the Plan (including discounts, rebates, payments in kind, or other premium differential mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program);

(c) The application of any pre-existing condition exclusion under the Plan; and

(d) Other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits.

If a Covered Individual seeks a benefit under the Plan that is conditioned on its medical appropriateness, and such determination depends on the Genetic Information of the individual, then the Plan is permitted to condition the benefit on the Genetic Information and that determination will not be within the meaning of Underwriting Purposes, provided that only the minimum amount of Genetic Information necessary to make the determination is requested. However, if a Covered Individual is not seeking a benefit under the Plan, this medical appropriateness exception to the definition of Underwriting Purposes will not apply.

Use. “Use” of PHI means the sharing, employment, application, utilization, examination or analysis of PHI by any Workforce Member or with another organization (such as that of a Business Associate) that maintains the PHI.

Workforce Member. A “Workforce Member” means any employee, volunteer, trainee, or other person whose work performance is under the direct control of SDIS, whether or not the person is paid by SDIS or the Plan, and whose duties and responsibilities necessitate access to PHI created or received under the Plan.

ARTICLE 3

Administrative Policies

3.1 Privacy Official and Contact Person.

(a) SDIS will appoint a person to serve as the Privacy Official with respect to the Plan. The Privacy Official will be responsible for the development and implementation of policies and procedures relating to use and disclosure of PHI. The Privacy Official will also serve as the contact person for Covered Individuals who have questions regarding the uses and disclosures of PHI that may be made by the Plan, and of the Covered Individual's rights and SDIS's legal duties with respect to PHI, unless SDIS appoints another person or office to serve as such.

3.2 Training.

(a) An individual who becomes a Workforce Member will receive training regarding these Privacy Policies. The training will be provided within a reasonable time after the individual assumes such position. The scope of the training will be as necessary and appropriate to permit the Workforce Member to carry out his or her Plan duties.

(b) In the event of a material change in these Privacy Policies, training will be provided to Workforce Members whose functions are affected by the change. Such training will be performed within a reasonable period of time after the change becomes effective.

(c) The training provided pursuant to this Section 3.2 will be documented as prescribed in Section 3.10.

3.3 Technical and Physical Safeguards.

(a) The Privacy Official will establish appropriate administrative, technical and physical safeguards to prevent PHI from being intentionally or unintentionally used or disclosed in violation of the HIPAA Privacy Rule.

(b) In regard to the establishment of administrative safeguards, consideration may be given to the following:

- (i) Personnel security
- (ii) Contingency plans
- (iii) Workforce Member termination procedures
- (iv) PHI training

(c) In regard to the establishment of technical safeguards, consideration may be given to the following:

- (i) Access control features
- (ii) Procedures for emergency access
- (iii) Role based access restrictions
- (iv) User identity authorization
- (v) Use of encryption

(d) In regard to the establishment of physical safeguards, consideration may be given to the following:

- (i) The locking of doors and filing cabinets
- (ii) Need to know procedures for personnel access
- (iii) Document storage and disposal procedures

3.4 Notice of Privacy Practices.

(a) The Privacy Official is responsible for developing and maintaining a “Notice of Privacy Practices” (the “Notice”). The Notice will be written in plain language and will include, among other disclosures that may be required by the HIPAA Privacy Rule, the following:

- (i) An explanation of the uses and disclosures of PHI that may be made by the Plan;
- (ii) A statement of the rights of Covered Individuals with respect to PHI, and a brief description of how a Covered Individual may exercise those rights;
- (iii) A statement that Covered Individuals may complain to the Privacy Official and to the HHS if they believe their privacy rights have been violated, and a brief description of how a Covered Individual may file a complaint with the Privacy Official; and
- (iv) The name, or title, and telephone number of the Privacy Official, or of such other person or office to contact for further information regarding the Plan’s Privacy Policies.

(b) An employee will be provided the Notice upon becoming covered under the Plan. Employees who later become enrolled will be provided the Notice at the time of enrollment. In the event of a material revision of the Notice, all employees then covered under the Plan will be provided the revised Notice (or information about the material revision and how to obtain the revised Notice) within 60 days of the revision, or as of such later date as may be allowed by the HHS. SDIS will also post the Notice on its intranet web site by the effective date of the material revision.

(c) A Covered Individual may receive a version of the Notice upon request at any time. No less frequently than once every three years, employees then covered under the Plan will be informed of the availability of the Notice and how to obtain the Notice.

(d) For purposes of this Section 3.4, an “employee covered under the Plan” includes a retired employee, a former employee receiving COBRA continuation coverage and an “alternate recipient” receiving coverage pursuant to a Qualified Medical Child Support Order.

(e) The Notice, and each revised Notice, will be maintained in accordance with the documentation provisions of Section 3.10 of these Privacy Policies.

3.5 Complaint Process.

(a) A Covered Individual who believes that the Plan is not complying with the HIPAA Privacy Rule, or who otherwise has concerns regarding the Plan’s Privacy Policies, may submit a complaint to the Privacy Official. In order for the complaint to be acted upon, it must satisfy the following requirements:

(i) The complaint must be filed in writing, either on paper or electronically;

(ii) The complaint must describe the acts or omissions believed to be in violation of the HIPAA Privacy Rule, or the other concerns regarding the Plan’s Privacy Policies; and

(iii) In the case of a complaint involving an act or omission of a privacy standard, the complaint must be filed within 180 days of when the complainant knew or should have known that the act or omission occurred.

(b) All complaints received the Privacy Official will be promptly reviewed. Within 30 days of the receipt of the complaint, the Privacy Official will make a determination regarding the complaint and notify the complainant in writing of the determination.

(c) If the Privacy Official determines that the complaint is without merit, or that no action warrants being taken, this disposition will be noted and the complainant so informed.

(d) If a breach of policy or procedure has resulted in an unauthorized use or disclosure of PHI, the Privacy Official will immediately implement steps to mitigate any potential harm to the affected Covered Individual.

(e) A Covered Individual who believes that the Plan is not complying with the HIPAA Privacy Rule may also file a complaint with the HHS. Complaints made to the HHS may be made in writing, and should be mailed or faxed directly to:

Regional Manager
Office for Civil Rights
U.S. Department of Health and Human Services
2201 Sixth Avenue – M/S: RX-11
Seattle, WA 98121-1831
FAX (206) 615-2297

(f) No officer, employee or agent of SDIS will intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any Covered Individual who files a complaint with the Privacy Official or with the HHS. An officer, employee or agent who discriminates or retaliates against a Covered Individual who files a complaint will be subject to disciplinary action, up to and including termination.

(g) All complaints submitted to the Privacy Official, and the documentation of the disposition of those complaints, will be subject to the documentation provisions of Section 3.10.

3.6 Sanctions for Violations of Privacy Policy. All Workforce Members who have access to PHI must comply with the Plan's Privacy Policies. Sanctions for using or disclosing PHI in violation of the Privacy Policies will be imposed in accordance with the discipline policy as set forth in SDIS's personnel policies, up to and including termination. Any discipline will be documented and copies will be kept in the Workforce Member's personnel file.

3.7 Mitigation of Inadvertent Disclosures. The Privacy Official will promptly investigate a report of an unauthorized use or disclosure of PHI. If the Privacy Official's investigation confirms the occurrence of an unauthorized use or disclosure of PHI in violation of these Privacy Policies, the Privacy Official will take positive reasonable action to minimize, to the extent possible, any known harmful effects resulting from the unauthorized use or disclosure and to assure no future unauthorized uses or disclosures. The Privacy Official will further take steps to correct, to the extent possible, known instances of harm. The Privacy Official will be obligated to notify an affected Covered Individual of an unauthorized use or disclosure of PHI only if such notification serves to mitigate the harmful effect of the disclosure, or the use or disclosure constitutes a reportable "Breach" as prescribed in Article 10.

3.8 No Intimidating or Retaliatory Acts.

(a) Neither SDIS nor any of its employees will intimidate, threaten, coerce, discriminate against or take other retaliatory action against any Covered Individual for the exercise by the Covered Individual of any right under, or for participation by the Covered Individual in any process established by, these Privacy Policies, including the filing of a complaint under Section 3.5.

(b) Neither SDIS nor any of its employees will intimidate, threaten, coerce, discriminate against or take other retaliatory action against any Covered Individual, or against any other person, for:

- (i) Filing a complaint with the HHS;
- (ii) Testifying, assisting or participating in an investigation, compliance review, proceeding or hearing involving the Plan's compliance with the HIPAA Privacy Rule; or
- (iii) Opposing any act or practice made unlawful by the HIPAA Privacy Rule, provided the Covered Individual or person has a good faith belief that the practice opposed is unlawful, and that the manner of the opposition is reasonable and does not involve an impermissible disclosure of PHI.

(c) Neither SDIS nor any of its employees will require a Covered Individual to waive any rights under the HIPAA Privacy Rule as a condition to enrollment in the Plan or to the payment or eligibility for benefits.

3.9 Plan Document Standard.

(a) PHI created or received by the Plan will not be disclosed to SDIS or to any of its employees unless the Plan document includes provisions that restricts the uses and disclosures of such information in a manner consistent with these Privacy Policies.

(b) The disclosure of such PHI to SDIS or any of its employees is further conditioned upon SDIS agreeing upon, and providing to the Privacy Official a written certification that the Plan document includes provisions that impose upon SDIS, the commitments to:

- (i) Not use or further disclose the PHI other than as permitted or required by the Plan document or as required by law;
- (ii) Ensure that any agents, including a subcontractor, to whom it provides PHI created or received by the Plan agree to the same restrictions and conditions that apply to SDIS with respect to such information;
- (iii) Not use or disclose the PHI for employment-related actions and decisions or in connection with any other benefit or employee benefit plan maintained by SDIS;
- (iv) Report to the Privacy Official any use or disclosure of PHI that is inconsistent with the uses or disclosures permitted under these Privacy Policies of which it becomes aware;
- (v) Allow each Covered Individual access to his or her own PHI, as prescribed in Article 6;

(vi) Allow Covered Individuals to request an amendment of their PHI, as prescribed in Article 7;

(vii) Make available to the Privacy Official the information required to provide an accounting of disclosures required under Article 8;

(viii) Make SDIS's internal practices, books, and records relating to the use and disclosure of PHI received from the Plan available to the HHS upon request for purposes of the agency's determination of the Plan's compliance with the HIPAA Privacy Rule; and

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

(c) In addition to the above, the Plan document must further include provisions described below.

(i) A description of those employees or classes of employees or other persons under the control of SDIS who are to have access to PHI of Covered Individuals. Such description will expressly identify any employee or person who receives PHI in the ordinary course of the person's employment or business duties.

(ii) Restrictions of such employees and other persons on the access to, and use of, PHI to matters necessary for the administration functions that SDIS performs for the Plan.

(iii) An effective mechanism for resolving any incidents of noncompliance of the provisions of the Plan document by such persons referred to in subsection (b) above.

3.10 Documentation Standard.

(a) The Plan will maintain, in written or in electronic form, the following:

(i) The HIPAA Privacy Policies adopted by SDIS, as may be amended from time to time;

(ii) The Notice of Privacy Practices described in Section 3.4;

(iii) Any agreement to the Covered Individual's request for a restriction on the use or disclosure of PHI, as prescribed in Section 5.1;

(iv) The Plan records that are available for access by Covered Individuals, as prescribed in Article 6;

(v) The titles of the persons or offices responsible for receiving and processing requests for access of PHI, or requests for amendment of PHI, as prescribed in Articles 6 and 7, respectively;

(vi) In regard to disclosures for which a Covered Individual is entitled to an accounting pursuant to Article 8, the information prescribed in Section 8.5(b);

(vii) Authorizations for release of PHI made pursuant to Section 4.4;

(viii) Complaints received, and the recordation of their disposition, if any, as prescribed in Section 3.5;

(ix) Any sanctions applied as a result of a Workforce Member having breached a provision of the Privacy Policies, as prescribed in Section 3.6; and

(x) Any other communication, action, activity or designation required by these Privacy Policies to be documented.

(b) The documentation will be maintained for no less than six years from the date the document was created or the date when it was last in effect, whichever is later.

ARTICLE 4

Use and Disclosure of Protected Health Information

4.1 General. SDIS and the Plan will use and disclose a Covered Individual's PHI only as follows:

- (a) Disclosures made to the Covered Individual;
- (b) For Payment or Health Care Operations purposes, as such terms are defined in Article 2, and as further discussed in Section 4.3;
- (c) Pursuant to the Covered Individual's authorization, as prescribed in Section 4.4;
- (d) For a purpose expressly permitted or required under Section 4.7;
- (e) In a manner that is incident to a permissive use or disclosure, provided that the minimum necessary standard of Section 4.8 has been satisfied in regard to such use or disclosure; or
- (f) When required to do so by the HHS in connection with a review of the Plan's compliance with the HIPAA Privacy Rule.

4.2 Prohibited Uses and Disclosures. Notwithstanding any other provision of this Article 4 to the contrary, the Plan may not Use or Disclose a Covered Individual's PHI that is Genetic Information, or for any Underwriting Purposes.

4.3 Payment or Operations Purposes. Subject to Section 4.2 above, the Plan may use or disclose PHI for its own Payment or Health Care Operations. For example, the Plan may provide health information to another health plan to coordinate the payment of benefits. The Plan may also use and disclose PHI to facilitate the administration and operation of the Plan, and to provide coverage and services to all individuals covered under the Plan. Accordingly, the Plan may use PHI in connection with eligibility and enrollment activities, medical review, case management, actuarial underwriting and legal services, audit services, fraud and abuse detection programs, planning and development programs such as cost management and general Plan administrative activities. The Plan may also disclose a Covered Individual's PHI in the following circumstances:

- (a) To a health care provider so as to assist in the provider's treatment activities;
- (b) To another health plan or a health care provider for the payment activities of that other plan or provider; and

(c) To another health plan or a health care provider for the health care operations activities of the plan or provider, if both the Plan and the other entity either has or had a relationship with the Covered Individual, the PHI pertains to such relationship and the disclosure is made for a purpose described below:

(i) Quality assessment and improvement activities, population based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives, or related functions that do not include treatment;

(ii) Reviewing the competence or qualifications of health care professionals, or evaluating practitioner, provider or health plan performance; or

(iii) Health care fraud and abuse detection or compliance.

4.4 Authorization for Release of PHI.

(a) Except as otherwise expressly permitted or required in these Privacy Policies, the Plan may not use or disclose a Covered Individual's PHI without an authorization that is valid under this Section 4.4. If the Plan obtains or receives a valid authorization, the use or disclosure by the Plan with respect to the PHI at issue must be consistent with such authorization. In no event may the Plan use or disclose a Covered Individual's Genetic Information for Underwriting Purposes, even if the Covered Individual signs an authorization allowing such use or disclosure.

(b) Notwithstanding any provision of these Privacy Policies to the contrary, the Plan must obtain an authorization for any Use or Disclosure of psychotherapy notes, except:

(i) To carry out the following treatment, payment, or health care operations:

(1) Use by the originator of the psychotherapy notes for treatment; and

(2) Use or Disclosure by SDIS or the Plan to defend itself in a legal action or other proceeding brought by a Covered Individual;

(ii) A Use or Disclosure to a health oversight agency or as required by law.

(c) An authorization is not valid if it has any of the following defects:

(i) The expiration date has passed or the expiration event is known by the Plan to have occurred;

(ii) The authorization is known by the Plan to have been revoked;

(iii) Any material information in the authorization is known by the Plan to be false; or

(iv) The authorization is incomplete or otherwise fails to include all the required elements.

(d) The Plan may condition an individual's enrollment in the Plan or eligibility for benefits on the individual providing an authorization, but only if the authorization is requested by the Plan prior to an individual's enrollment in the Plan and is sought either for Plan eligibility or enrollment determinations relating to the individual or for underwriting or risk rating determinations. However, the authorization may not be combined with any other document.

(e) A Covered Individual may revoke an authorization at any time. To be effective, the revocation must be in writing and submitted to the Privacy Official. A revocation will not be effective to the extent that the Plan or other disclosing entity has taken action in reliance of the authorization. A revocation will also not be effective with respect to an authorization obtained as a condition of obtaining insurance coverage, to the extent that another law provides the insurer with the right to contest a claim under the insurance policy.

(f) The Plan will retain each signed authorization in accordance with the documentation standards prescribed in Section 3.10. In addition, the Plan must provide the Covered Individual with a copy of the signed authorization.

4.5 Disclosures to Involved Persons.

(a) The Plan may use or disclose a Covered Individual's PHI without the written authorization of the Covered Individual if the Covered Individual is informed in advance of the use or disclosure and has the opportunity to agree to or prohibit or restrict the disclosure in accordance with the applicable requirements of this Section 4.5. The Plan may orally inform the Covered Individual of, and obtain the Covered Individual's oral agreement or objection to, a use or disclosure.

(b) Subject to the conditions prescribed in subsections (c) and (d) below, the Plan may disclose to a family member, other relative, or a close personal friend of the Covered Individual, or any other person identified by the Covered Individual, PHI that is directly relevant to such person's involvement with the individual's care or payment related to the Covered Individual's health care.

(c) If the Covered Individual is present for, or otherwise available prior to, a use or disclosure permitted under subsection (b) above and has the capacity to make health care decisions, the Plan may use or disclose PHI if it:

(i) Obtains the Covered Individual's agreement to the use or disclosure;

(ii) Provides the Covered Individual with the opportunity to object to the use or disclosure and the Covered Individual does not express an objection; or

(iii) Reasonably infers from the circumstances, based on the exercise of professional judgment that the Covered Individual does not object to the use or disclosure.

(d) If the Covered Individual is not present for, or the opportunity to agree or object to the use or disclosure cannot practically be provided because of the Covered Individual's incapacity or an emergency circumstance, the Plan may, in the exercise of professional judgment, determine whether the use or disclosure is in the best interests of the Covered Individual and, if so, disclose only the PHI that is directly relevant to the person's involvement with the Covered Individual's health care.

(e) If the Covered Individual is deceased, the Plan may disclose to a family member, or other persons who were involved in the individual's care or payment for health care prior to the Covered Individual's death, PHI of the Covered Individual that is relevant to such person's involvement, unless doing so is inconsistent with any prior expressed preference of the Covered Individual that is known to the Plan.

4.6 De-Identified Information.

(a) Health information that does not include any of the identifiers listed in subsection (b) below with respect to any Covered Individual, or of relatives, employers or household members of the Covered Individual, is not PHI, and thus may be used or disclosed without the Covered Individual's authorization, but only if:

(i) There is no reasonable basis to believe that the information can be used to identify a Covered Individual; and

(ii) The Plan does not have actual knowledge that the information could be used alone or in combination with other information to identify a Covered Individual who is the subject of the information.

(b) The identifiers referred to in subsection (a) above are as follows:

- Names;
- All geographic subdivisions smaller than a state, including street address, Company, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:
- The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
- The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000;
- All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;

- Telephone numbers;
- Fax numbers;
- Electronic mail addresses;
- Social security numbers;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate and license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints;
- Full face photographic images and any comparable images; and
- Any other unique identifying number, characteristic or code.

4.7 Other Sanctioned Disclosures. The Plan may use or disclose PHI in the situations prescribed below.

(a) The Plan may use and disclose a Covered Individual's health information to inform a Covered Individual of possible treatment options or alternatives that may be of interest to the Covered Individual.

(b) The Plan may use and disclose a Covered Individual's health information to inform the individual of health related benefits or services that may be of interest to the Covered Individual.

(c) The Plan may disclose a Covered Individual's health information in response to a court or administrative order, a subpoena, warrant, discovery request or other lawful process.

(d) The Plan may disclose a Covered Individual's health information if asked to do so by a law enforcement official. For example, the Plan may disclose health information to a police officer if needed to help find or identify a missing person.

(e) The Plan may disclose a Covered Individual's health information as necessary to comply with applicable workers' compensation or similar laws.

(f) The Plan may use and disclose a Covered Individual's health information when necessary to prevent a serious threat to the individual's health and safety or to the health and safety of the public or another person.

(g) The Plan may disclose health information about a Covered Individual for public health activities, such as providing information to an authorized public health authority for the purpose of preventing or controlling a disease, injury or disability.

(h) The Plan may disclose a Covered Individual's health information to a health oversight agency for audits, investigations, inspections and licensure necessary for the government to monitor the health care system and government programs or to ascertain compliance with applicable civil rights laws.

(i) The Plan may use or disclose a Covered Individual's health information to facilitate specified government functions related to the military and veterans, national security and intelligence activities, protective services for the President and others and correctional institutions and inmates.

(j) The Plan may disclose a Covered Individual's health information to a coroner or medical examiner (for example, to assist in identifying the cause of a person's death).

(k) If a Covered Individual is an organ donor, the Plan may release PHI to organizations that handle organ procurement or organ, eye or tissue transplantation or to an organ donation bank, as necessary to facilitate organ or tissue donation and transplantation.

(l) The Plan will disclose PHI about a Covered Individual when required to do so by federal, state or local law, but only to the extent of the relevant requirements of such law.

4.8 "Minimum Necessary" Standard.

(a) When using or disclosing PHI, or when requesting PHI from another health plan or health care provider, the Plan will make reasonable efforts to limit the PHI used or disclosed, or the PHI being requested, to the minimum necessary to accomplish the intended purpose.

(b) The minimum necessary standard does not apply to any of the following:

(i) Disclosures to or requests by a health care provider for treatment purposes;

(ii) Uses or disclosures made to the Covered Individual pursuant to the individual's request;

(iii) Uses or disclosures made pursuant to an authorization, as prescribed in Section 4.4;

(iv) Disclosures made to the HHS in connection with its review of the Plan's compliance with the HIPAA Privacy Rule;

(v) Uses or disclosures that are required by law; and

(vi) Uses or disclosures that are required in order for the Plan to comply with the HIPAA Privacy Rule.

(c) The Privacy Official will identify the Workforce Members needing access to PHI, and who thus may receive PHI in order to carry out their duties.

(d) The categories of PHI to which access is required by such Workforce Members Needing Access are information relating to Payment and Health Care Operations (each as defined in Article 2), and any others that the Privacy Official determines are needed by such individuals to carry out their duties under the Plan.

(e) The Plan can assume (if such assumption is reasonable) that in the situations described below, the requestor has made a proper determination and is asking only for the minimum necessary information needed for the stated purpose. Consequently, the Plan is not required to make a supplemental determination of the minimum necessary information to be disclosed.

(i) A request for PHI made by a health plan or by a health care provider;

(ii) A request for PHI made by a professional who is a Workforce Member or a Business Associate of the Plan for the purpose of providing legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, financial or other professional services to the Plan, if the professional represents that the information requested is the minimum necessary for the stated purpose; or

(iii) Disclosures to public officials as permitted under Section 4.7, if the public official represents that the information requested is the minimum necessary for the stated purpose.

4.9 Disclosures Regarding Minors, Dependents and Descendants.

(a) As in regard to a Covered Individual who is an unemancipated minor, the Plan may disclose the PHI of the minor, and may provide access of the minor's PHI in accordance with Article 6, to the minor's parent, guardian or other person acting in loco parentis unless prohibited by applicable state law.

(b) A person having lawful authority to act in regard to health care decisions on behalf of a Covered Individual who is an adult or an emancipated minor, or an executor, administrator or other person having lawful authority to act on behalf of a deceased Covered Individual or of the Covered Individual's estate, must be treated by the Plan as the Covered Individual's personal representative with respect to PHI relevant to such personal representation. Consequently, disclosures of the Covered Individual's PHI may be made to the personal representative. In addition, a personal representative may exercise on behalf of the Covered Individual any of the rights prescribed in Article 5, 6, 7 and 8.

(c) Notwithstanding a state law or any foregoing provision of this Section 4.9 to the contrary, the Plan may choose not to treat a person as the personal representative of a Covered Individual if:

(i) The Plan has a reasonable belief that:

(1) The Covered Individual has been or may be subjected to domestic violence, abuse or neglect by such person; or

(2) Treating such person as the personal representative could endanger the Covered Individual; and

(ii) The Plan, in the exercise of professional judgment, decides that it is not in the best interest of the Covered Individual to treat the person as the Covered Individual's personal representative.

4.10 Verification of Identity and Authority.

(a) Except as with respect to disclosures made pursuant to Section 4.5, the Plan will verify the identity of a person requesting PHI and the authority of such person to have access to PHI, if the identity or other such authority is not known to the Plan.

(b) The identity of a Covered Individual requesting information or other access to the individual's own PHI can be verified by any of the following methods:

(i) Asking for the Covered Individual's birth date or social security number;

(ii) Calling back the individual at the phone number in the Plan records;

(iii) Inspection of a form of photo identification, such as a driver's license; or

(iv) Any other method reasonably designed to verify the identity of the requestor.

(c) Where the person requesting the PHI is a public official, the Plan may rely, if such reliance is reasonable under the circumstances, on any of the following to verify that the requestor is a public official or a person acting on behalf of the public official:

(i) If the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status;

(ii) If the request is in writing, the request is on the appropriate government letterhead; or

(iii) If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services or memorandum of understanding, that establishes that the person is acting on behalf of the public official.

(d) The Plan may rely, if such reliance is reasonable under the circumstances, on any of the following to verify the authority of the public official or a person acting on behalf of the public official:

(i) A written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority; or

(ii) If a request is made pursuant to legal process, warrant, subpoena, order or other legal process issued by a grand jury or a judicial or administrative tribunal, it is presumed to constitute legal authority.

(e) The Plan is not required to verify a person's identity or authority if the PHI is disclosed for the purpose of preventing or lessening a serious and imminent threat to the health or safety, and the person to whom the PHI is being disclosed is reasonably able to prevent or lessen the threat.

(f) The Plan may verify the identity and authority of a Covered Individual's personal representatives, if not known to the Plan, by:

(i) Requiring a power of attorney;

(ii) Asking questions to determine that an adult acting for a young child has the requisite relationship to the child; or

(iii) Any other method reasonably designed to ascertain such identity or authority.

ARTICLE 5

Requests for Privacy Protections

5.1 Requested Restriction of Uses and Disclosures.

(a) A Covered Individual may request restrictions on the extent by which the Covered Individual's PHI is used or disclosed by the Plan for treatment, payment or health care operation purposes. A Covered Individual also has the right to request a restriction on the Plan's disclosure of his or her PHI to someone involved in the payment of the individual's care. For example, a Covered Individual may request that the Plan not disclose to a family member information regarding a particular surgery undertaken by the Covered Individual. However, the Plan is not required to agree to the request.

(b) A request for restrictions must be made in writing to the Privacy Official, and must identify:

(i) The specific PHI requested to be restricted;

(ii) Whether the requested restriction applies to the use or the disclosure of the PHI, or both; and

(iii) To whom the Covered Individual wants the restrictions to apply (for example, disclosure to the Covered Individual's spouse).

(c) The Privacy Official's decision to accommodate the Covered Individual's request for restrictions on the use and disclosure will be made on the basis of the feasibility and Plan administration implications of the requested restriction. The Privacy Official may choose not to approve the requested restrictions. A decision of the Privacy Official to deny the request for restrictions will be final and is not subject to appeal by the Covered Individual. The Privacy Official will promptly notify the Covered Individual of the decision regarding the request for restrictions on the use or disclosure of PHI.

(d) If the Privacy Official agrees to a restriction under this Section 5.1, then neither the Plan, nor a Business Associate on behalf of the Plan, may use or disclose the PHI at issue in violation of such restriction. However, an agreed upon restriction is not effective to prevent uses or disclosures permitted or required under Section 4.6.

(e) The Plan may terminate its agreement to a restriction, including with respect to PHI created or received before the termination, if the Covered Individual agrees to or requests the termination in writing, or the Covered Individual orally agrees to the termination and the oral agreement is documented. The Plan may also terminate its agreement to a restriction by notifying the Covered Individual of such termination. However, the termination will be effective only with respect to PHI created or received after notice of the termination is provided to the Covered Individual. The notice of termination may either be in writing, or orally if such oral communication is documented.

(f) Any agreement to a restriction of the use or disclosure of PHI, or the termination of such an agreement, will be subject to the documentation provisions of Section 3.10.

5.2 Request for Confidential Communications.

(a) Covered Individuals have the right to request that the Plan communicate with them in a certain way if they feel the disclosure of their PHI could endanger them. For example, a Covered Individual may ask that the Plan only communicate with the individual at a certain telephone number or by email.

(b) If a Covered Individual wishes to receive communications in a confidential manner, the individual must make a request in writing to the Privacy Official. The request must specify how or where the Covered Individual wishes to be contacted. The request must also include a statement that the disclosure of all or part of the PHI to which the request pertains could endanger the Covered Individual. The Plan will attempt to honor reasonable requests for confidential communications.

ARTICLE 6

Right of Access to Protected Health Information

6.1 General Right of Access. Except as otherwise provided in Section 6.2, a Covered Individual has a right of access to inspect and obtain a copy of (i.e., to have “access” to) PHI about the Covered Individual maintained by the Plan for as long as the PHI is maintained by the Plan. All requests for access must be submitted in writing to the Privacy Official.

6.2 Non-Appealable Denials of Access. The Privacy Official will deny a Covered Individual access to PHI in the following circumstances:

- (a) The PHI has been compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative action or proceeding; or
- (b) The PHI was obtained from someone other than a health care provider under a promise of confidentiality, and the access requested would be reasonably likely to reveal the source of the information.

6.3 Reviewable Denials of Access.

(a) The Privacy Official will tentatively deny a Covered Individual’s access to PHI maintained by the Plan in the following circumstances:

- (i) A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the Covered Individual or another person;

- (ii) The PHI makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or

- (iii) The request for access is made by the Covered Individual’s personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the Covered Individual or another person.

(b) If access is denied on a ground permitted under subsection (a) above, the Covered Individual has the right to have the denial reviewed by a licensed health care professional who is designated by the Plan to act as a reviewing official and who did not participate in the original decision to deny the request.

6.4 Responding to Request.

(a) The Privacy Official must respond to a Covered Individual's request for access no later than 30 days after the receipt of the request. If the Privacy Official grants the request, in whole or in part, the Covered Individual must be informed, either in writing or orally, of the approval of the request and then provided the approved access, all within the 30 day time limit. If the Privacy Official denies the request, in whole or in part, the Privacy Official must timely provide the Covered Individual with a written denial as prescribed in Section 6.7.

(b) If the request for access is for PHI that is not maintained or accessible to the Privacy Official on site, the Privacy Official must take an action required by subsection (a) above no later than 60 days from the receipt of such a request.

(c) If the Privacy Official is unable to approve, or otherwise accommodate, the request for access within the applicable 30 or 60 day time limit, the Privacy Official may extend the time for such actions by no more than 30 days, provided that within the otherwise applicable time limit, the Privacy Official provides the Covered Individual with a written statement of the reasons for the delay and the date by which the Privacy Official will complete the action on the request. Only one such extension of time is permitted.

6.5 Form of Access.

(a) A Covered Individual whose request for access to PHI has been approved must be provided such access in the form or format requested by the Covered Individual, if it is readily producible in such form or format. If not so readily producible, then it must be provided in readable hard copy form, or in such other form or format as agreed to by the Privacy Official and the Covered Individual.

(b) If the PHI that is the subject of the request for access is maintained in one or more designated record sets electronically, and if the Covered Individual requests an electronic copy of such information, the Plan must provide the Covered Individual with access to the PHI in the electronic form and format requested by the Covered Individual, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by the Privacy Official entity and the Covered Individual.

(c) In lieu of providing a Covered Individual with access to the PHI, the Privacy Official may provide the Covered Individual with a summary of the requested PHI, or may provide an explanation of the requested PHI, but only if the Covered Individual agrees in advance to such a summary of explanation and the Covered Individual further agrees in advance to the fees imposed, if any, by the Plan for such summary or explanation.

6.6 Fees. If a Covered Individual requests a copy of the PHI or agrees to a summary or explanation of such PHI, the Plan may impose a reasonable, cost based fee, provided that the fee includes only the cost of:

(a) Labor for copying or creating the PHI requested by the Covered Individual, whether in paper form or electronic media;

(b) Supplies for creating the paper copy, or electronic media if the Covered Individual requests an electronic copy;

(c) Postage, when the Covered Individual has requested the cost, or the summary or explanation, be mailed; and

(d) Preparing an explanation or summary of the PHI, if agreed to by the Covered Individual as prescribed in Section 6.5(c).

6.7 Access Denial Procedures. If a Covered Individual's request for access to the PHI is denied, in whole or in part, the Plan must comply with the procedures set forth below.

(a) The Plan must, to the extent possible, give the Covered Individual access to any other requested PHI, after excluding the PHI as to which the Plan has a ground to deny access.

(b) The Plan must provide a timely, written denial to the Covered Individual. The denial must be written in plain language and provide the following:

(i) The basis for the denial;

(ii) If applicable, a statement of the Covered Individual's access denial review rights, including a description of how the Covered Individual may exercise such review rights; and

(iii) A description of how the Covered Individual may complain to the Privacy Official, or to the HHS, pursuant to the procedures set forth in Section 3.5. The description must include the name, or title, and telephone number of the Privacy Official, or other contact person or office designated in Section 3.1.

6.8 Redirection of Requests. If the Plan does not maintain the PHI that is the subject of the Covered Individual's request for access, but the Plan knows where the requested information is maintained, the Plan must inform the Covered Individual where to direct the request for access.

6.9 Documentation. All enrollment, payment, claims adjudication, and case or medical management systems records maintained by or for the Plan, and any other records used, in whole or in part, by or for the Plan to make decisions regarding Covered Individuals which are available for access by Covered Individuals pursuant to this Article 6 will be documented and maintained in accordance with the documentation standards prescribed by Section 3.10.

ARTICLE 7

Amendment of Protected Health Information

7.1 **Right to Amend.** A Covered Individual has the right to have the Plan revise, correct or clarify (i.e., “amend”) PHI or a record about the Covered Individual’s PHI maintained by the Plan for as long as the Plan maintains the PHI or record. Requests for an amendment of PHI must be made to the Privacy Official in writing and must state a reason to support the requested amendment.

7.2 **Grounds for Denial.** The Plan may deny a Covered Individual’s request for amendment if the Privacy Official determines that the PHI or record that is the subject of the request:

- (a) Was not created by the Plan, unless the Covered Individual provides a reasonable basis to believe that the originator of the PHI is no longer available to act on the requested amendment;
- (b) Is not part of the Plan records;
- (c) Is PHI that is not eligible for access pursuant to Section 6.2; or
- (d) Is in fact accurate and complete.

7.3 **Timing of Action.** The Privacy Official must approve or deny the Covered Individual’s request for an amendment no later than 60 days after receipt of such a request. If the Privacy Official is unable to act on the amendment within the 60-day period, the Privacy Official may extend the time for such action by no more than 30 days, but only if prior to the end of the otherwise applicable 60-day deadline, the Privacy Official provides the Covered Individual with a written statement of the reasons for the delay and the date by which the Privacy Official will complete the action on the request. Only one such extension of time is permitted.

7.4 **Effecting the Amendment.** If the Privacy Official determines that the request for an amendment of a Covered Individual’s PHI should be approved, in whole or in part, then the amendment will be effected in accordance with the requirements set forth below.

- (a) The Plan must timely inform the Covered Individual that the request for the PHI amendment is approved.
- (b) The Plan must make the appropriate amendment to the PHI or related Plan records. At a minimum, the scope of this amendment requires identifying Plan records that are affected by the amendment, and appending or otherwise providing a link to the location of the amendment.
- (c) The Plan must obtain the Covered Individual’s identification of, and agreement to have the Plan notify, the relevant persons to whom the amendment needs to be shared as prescribed in subsection (d) below.

(d) The Plan must make reasonable efforts to inform and provide the amendment within a reasonable time to:

(i) Persons identified by the Covered Individual as having received PHI about the Covered Individual and needing the amendment; and

(ii) Persons, including Business Associates, that the Plan knows possess the PHI that is the subject of the amendment, and that may have relied, or could foreseeably rely, on such information to the detriment of the Covered Individual.

7.5 Denial of Amendment Request. If the Privacy Official denies, in whole or in part, a Covered Individual's request for an amendment to the individual's PHI, then the Privacy Official must provide the Covered Individual with a written notice of denial within the time period prescribed in Section 7.3 above. The notice of denial must be written in plain language, and must contain each of the following elements:

(a) An explanation of the basis for the denial;

(b) The Covered Individual's right to submit a written statement disagreeing with the denial, and the manner by which the Covered Individual may file such a statement;

(c) A notice that, if the Covered Individual does not submit a statement of disagreement, the Covered Individual may request that the Plan provide, with any future disclosures by the Plan of the PHI that is the subject of the requested amendment, a copy of the Covered Individual's request for amendment and the request denial; and

(d) A description of how the Covered Individual may complain to the Plan pursuant to the complaint procedures prescribed in Section 3.5. The description must include the name, or title, and telephone number of the Privacy Official, or such other contact person or office designated in Section 3.1(c).

7.6 Statement of Disagreement.

(a) A Covered Individual whose request for amendment has been denied may submit to the Privacy Official a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement. The Privacy Official may reasonably limit the length of a statement of disagreement.

(b) The Privacy Official may, but is not required to, prepare a written rebuttal to the Covered Individual's statement of disagreement. If such a rebuttal is prepared, the Privacy Official must provide a copy to the Covered Individual who submitted the statement of disagreement.

7.7 Notation of Disagreement. If a Covered Individual's request for amendment of PHI is denied, the Plan must, as appropriate, identify the PHI or other Plan record that is the subject of the denied amendment, and then append or otherwise link to such PHI or record the following:

- (a) The Covered Individual's request for an amendment;
- (b) The Privacy Official's denial of the request;
- (c) The Covered Individual's statement of disagreement, if any; and
- (d) The Privacy Official's rebuttal, if any, to the statement of disagreement.

7.8 Effect of Denial on Subsequent Disclosures. If a Covered Individual's request for amendment of PHI is denied, then future disclosures of the Covered Individual's PHI will be subject to the rules prescribed below.

(a) If a statement of disagreement has been submitted to the Covered Individual, the Plan must include with any subsequent disclosure of the PHI to which the disagreement relates either:

- (i) The material appended or linked to the Covered Individual's PHI or record; or
- (ii) At the election of the Plan, an accurate summary of any such information.

(b) If the Covered Individual has not submitted a written statement of disagreement, the Plan must include, with any subsequent disclosure of the PHI at issue, the Covered Individual's request for amendment and its denial, or an accurate summary of such information, but only if the Covered Individual has requested such action in accordance with Section 7.5(c).

(c) If a subsequent disclosure described above is made using a standard electronic transaction that does not permit the additional material to be included with the disclosure, the Plan may separately transmit the requisite material to the recipient of the standard transaction.

7.9 External Notice of Amendment. If the Plan is informed by another health plan or a health care provider of an amendment to a Covered Individual's PHI, the Plan must amend its records as prescribed in Section 7.4.

7.10 Documentation. The Plan must document the titles of the persons or offices responsible for receiving and processing requests for amendments by Covered Individuals, and retain the documentation in accordance with Section 3.10.

ARTICLE 8

Accounting of Disclosures of Protected Health Information

8.1 **Right to an Accounting.** Except as otherwise provided in this Article 8, a Covered Individual has a right to receive an accounting of disclosures of PHI made by the Plan during the six year period preceding the date on which the accounting is requested.

8.2 **Accountable Disclosures.** Except as otherwise provided in Section 8.3 below, a Covered Individual has the right to an accounting of disclosures of the Covered Individual's PHI made in the following circumstances:

- (a) In response to a court or administrative order, subpoena, warrant, discovery request or other lawful process;
- (b) To a law enforcement official;
- (c) To comply with applicable workers' compensation or similar laws;
- (d) To prevent a serious threat to a Covered Individual's health and safety or to the health and safety of the public or another person;
- (e) For public health activities, such as providing information to an authorized public health authority for the purpose of preventing or controlling a disease, injury or disability;
- (f) To a health oversight agency for audits, investigations, inspections and licensure necessary for the government to monitor the health care system and government programs or to ascertain compliance with applicable civil rights laws;
- (g) To facilitate specified government functions related to the military and veterans, or for protective services for the President and others;
- (h) To a coroner or medical examiner (for example, to assist in identifying the cause of a person's death);
- (i) To an organization that handles organ procurement or organ, eye or tissue transplantation or to an organ donation bank, as necessary to facilitate organ or tissue donation and transplantation; or
- (j) When required to do so by federal, state or local law.

8.3 **Ineligible Disclosures.** The Plan is not required to provide an accounting of any disclosures made under the following circumstances:

- (a) To carry out Payment and Health Care Operations (as those terms are defined in Article 2);

(b) To Covered Individuals regarding the Covered Individual's own PHI, including to provide information regarding possible treatment options or alternatives, or health related benefits or services, that may be of interest to the Covered Individual;

(c) Pursuant to an authorization, as prescribed in Section 4.3;

(d) To persons involved in the Covered Individual's care or other notification purposes, as provided in Section 4.4;

(e) Incident to a use or disclosure permitted or required to be made pursuant to Section 4.6;

(f) In a form that excluded all identifiers with respect to the Covered Individual, as prescribed in Section 4.5;

(g) For national security or intelligence purposes;

(h) To correctional institutions or other law enforcement custodial officials; or

(i) Disclosures made more than six years prior to the date of the accounting request.

8.4 Temporary Suspension of Accountings.

(a) The Plan must temporarily suspend a Covered Individual's right to receive an accounting of disclosures made to a health oversight agency or law enforcement official for the time specified by such agency or official if such agency or official provides the Plan with a written statement that such an accounting to the individual would be reasonably likely to impede the agency's activities and specifying the time for which such a suspension is required.

(b) If the statement of the agency or official is made orally, the Plan must:

(i) Document the statement, including the identity of the agency or official making the statement;

(ii) Temporarily suspend the Covered Individual's right to an accounting of disclosures subject to the statement; and

(iii) Limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement is submitted during that time.

8.5 Content of the Accounting. The written accounting to be provided to a Covered Individual must comply with the requirements prescribed below.

(a) The accounting must include disclosures of PHI that occurred during the six year period (or such shorter time period as requested by the Covered Individual) prior to the date of the request for an accounting, including disclosures to or by Business Associates of the Plan.

- (b) The accounting must include for each disclosure:
 - (i) The date of the disclosure;
 - (ii) The name of the entity or person who received the PHI and, if known, the address of such entity or person;
 - (iii) A brief description of the PHI disclosed; and
 - (iv) A brief statement of the purpose of the disclosure that reasonably informs the Covered Individual of the basis for the disclosure, or, in lieu of such statement, a copy of a written request for a disclosure.
- (c) If during the period covered by the accounting the Plan has made multiple disclosures of PHI to the same person or entity for a single purpose, the accounting may, with respect to such multiple disclosures, merely provide:
 - (i) The information required by subsection (b) above for the first disclosure during the accounting period;
 - (ii) The frequency, periodicity or number of the disclosures made during the accounting period; and
 - (iii) The date of the last such disclosure during the accounting period.

8.6 Deadline for Providing Accounting.

(a) In general, the Plan must provide a Covered Individual with the requested accounting no later than 60 days after receipt of such a request. However, if the Plan is unable to provide the accounting within such time period, the Plan may extend the time to provide the accounting by no more than 30 additional days, provided that prior to the end of the generally applicable 30-day period, the Covered Individual is provided with a written statement of the reasons for the delay and the date by which the Plan will provide the requested accounting. Only one such extension of time is permitted.

(b) The Plan must provide the first accounting to a Covered Individual in any 12 month period without charge. The Plan may impose a reasonable, cost based fee for each subsequent request for an accounting by the same Covered Individual within the 12-month period, provided that the Plan informs the individual in advance of the fee and provides the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

8.7 Documentation. The following must be documented by the Plan and retained under the standards prescribed under Section 3.10:

(a) The information required to be included in an accounting pursuant to Section 8.5(b);

(b) The written statement of accounting that is provided to the Covered Individual; and

(c) The Privacy Official, or the titles of any other persons or offices responsible for receiving and processing requests for an accounting by Covered Individuals.

ARTICLE 9

Disclosures to Business Associates

9.1 **Restrictions on Disclosures.** The Plan and Workforce Members will not disclose PHI to any Business Associate in the absence of a written contract that assures that the Business Associate will:

- (a) Use the information only for the purposes for which the Business Associate was engaged by the Plan;
- (b) Safeguard the information from misuse; and
- (c) Assist the Plan to comply with the Plan's duties to provide Covered Individuals with access to their PHI and a history of certain disclosures.

9.2 **Business Associates.**

(a) A "Business Associate" with respect to the Plan is an organization or a person (other than a Workforce Member) who, on behalf of the Plan, performs, or assists in the performance of, a function or activity involving the use or disclosure of PHI. Examples of such functions and activities are:

- (i) Claims processing or administration;
- (ii) Plan administration;
- (iii) Data analysis;
- (iv) Utilization review;
- (v) Quality assurance;
- (vi) Billing;
- (vii) Benefit management;
- (viii) Practice management; and
- (ix) Any other activity regulated by the HIPAA Privacy Rule.

(b) A Business Associate may also be an organization or a person (other than a Workforce Member) who provides any of the following services for or to the Plan, where the provision of the service involves the disclosure of PHI to the Business Associate from the Plan (or to another Business Associate of the Plan):

- (i) Legal;
- (ii) Actuarial;

- (iii) Accounting;
- (iv) Consulting;
- (v) Data aggregation;
- (vi) Management;
- (vii) Administration;
- (viii) Accreditation; or
- (ix) Financial services.

9.3 Managing Business Associate Contracts. The Privacy Official will be responsible for managing all contracts with Business Associates. Such management responsibilities include assuring that contracts are executed for all Business Associates and that contracts are current and in compliance with the requirements of the HIPAA Privacy Rule. No changes or modifications to the language of the contract form may be made without prior review and authorization by the Privacy Official.

9.4 Plan Responsibilities.

(a) The Plan will provide to each Business Associate the necessary information and documentation to assure that the Business Associate complies with the Privacy Policies of the Plan. The Privacy Official will be responsible for coordinating the flow of information between the Plan and Business Associates.

(b) The Plan will provide each Business Associate with appropriate documentation regarding requiring authorization or restrictions related to the use and disclosure of a Covered Individual's PHI. Each Business Associate will also be informed in writing of any changes in, or withdrawal of, any such authorization or restriction.

9.5 Business Associate's Responsibilities.

(a) At the request of the Plan, a Business Associate will provide access to a Covered Individual's PHI by a Workforce Member, or by a Covered Individual to whom such PHI relates, in order for the Plan to comply with a request for access to such PHI, as required under Article 6.

(b) At the request of the Privacy Official, a Business Associate will make any amendments to PHI that the Privacy Official approves and directs in response to a Covered Individual's request for amendment, as prescribed under Article 7.

(c) In the event the Business Associate relationship is terminated, the Business Associate will return or destroy all PHI in its possession, if feasible. The Business Associate will also recover any PHI in the possession of its subcontractors or agents. If it is not feasible to recover the PHI, the Business Associate will notify the Privacy Official in writing.

9.6 Unauthorized Use or Disclosure. The contract entered into with each Business Associate will provide that the Business Associate is obligated to notify the Plan when any unauthorized use or disclosure of PHI has occurred by the Business Associate. If the Plan becomes aware of a pattern or practice of the Business Associate that constitutes a material breach or violation of the Business Associate's obligations under the contract, the Plan will take reasonable steps to cure the breach or to end the violation. Reasonable steps will vary with the circumstances and the nature of the relationship. The Privacy Official will coordinate activities to address the violation.

9.7 No Liability for the Actions of Business Associates. The Plan, SDIS and employees of SDIS will not be liable for a Business Associate's violations of the HIPAA Privacy Rule. The Plan, SDIS and employees of SDIS will not be required to actively monitor or oversee the means by which the Business Associate carries out safeguards of PHI or the extent to which the Business Associate abides by the requirements of the Business Associate's contract with the Plan.

ARTICLE 10

Notification in the Case of Breach

10.1 General. In the event that SDIS discovers any Breach of Unsecured PHI, SDIS will notify each Covered Individual whose Unsecured PHI has been, or is reasonably believed by SDIS to have been, accessed, acquired, or disclosed as a result of such Breach.

10.2 Definitions. When used in this Article 10, the following terms have the meanings set forth below.

(a) Unsecured PHI. “Unsecured PHI” means PHI with respect to any Covered Individual that has not been rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of technology or methodology specified in guidance issued by the HHS.

(b) Breach. “Breach” means the acquisition, access, use or disclosure in a manner not permitted under the HIPAA Privacy Rule of Unsecured PHI that compromises the security or privacy of such information. Notwithstanding the foregoing, the term “Breach” does not include:

(i) Any unintentional acquisition, access, or use of Unsecured PHI by a Workforce Member or individual acting under the authority of the Plan or a Business Associate if:

(1) Such acquisition, access, or use was made in good faith and within the course and scope of the employment or other professional relationship of such Workforce Member or individual; and

(2) Such information is not further used or disclosed in a manner not otherwise permitted under the HIPAA Privacy Rule; or

(ii) Any inadvertent disclosure from an individual who is otherwise authorized to access Unsecured PHI at a facility operated by SDIS or a Business Associate to another similarly authorized individual at the same facility (or at the facility of an insurance carrier or other organized health care arrangement member), and such information is not further used, or disclosed in a manner not otherwise permitted under the HIPAA Privacy Rule; and

(iii) A disclosure of Unsecured PHI where the Plan or Business Associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

10.3 Presumption of Breach. An acquisition, access, use or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule is presumed to be a Breach unless the Plan or Business Associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment that, as a minimum, takes into account the following factors:

- (a) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
- (b) The unauthorized person who used the PHI or to whom the disclosure was made;
- (c) Whether the PHI was actually acquired or viewed; and
- (d) The extent to which the risk to the PHI has been mitigated.

10.4 Notice to Covered Individuals. The notice required to be provided to a Covered Individual under Section 10.2 with respect to a Breach of Unsecured PHI will be provided promptly and in the form prescribed below.

(a) Written notification by first-class U.S. Mail to the Covered Individual (or the next of kin of the Covered Individual if the Covered Individual is deceased) at the last known address of the Covered Individual (or the next of kin). Electronic notification will also satisfy this requirement if agreed upon by the Covered Individual (or the next of kin). The notification may be provided in one or more mailings as information regarding the Breach is made available.

(b) In the case in which there is insufficient, or out-of-date, contact information (including phone number, e-mail address, or any other form of appropriate communication) that precludes direct written (or electronic, if specified by the Covered Individual) notification to the Covered Individual, a substitute form of notice will be provided.

(c) For Breaches involving fewer than ten Covered Individuals for which there is insufficient or out-of-date contact information, the substitute notice may be provided by an alternative form of written notice, by telephone, or by other means.

(d) For Breaches involving ten or more Covered Individuals for which there is insufficient or out-of-date contact information, substitute notification will be made for a period of 90 days through a conspicuous posting on SDIS' web site, or in major print or broadcast media outlets in the geographic areas where the Covered Individuals affected by the Breach likely reside. Such a notice will include a toll-free phone number that remains active for at least 90 days where a Covered Individual can learn whether or not the Covered Individual's Unsecured PHI is possibly included in the Breach.

(e) In any case deemed by SDIS to require urgency because of possible imminent misuse of Unsecured PHI, SDIS may provide information to Covered Individuals by telephone or other means, as appropriate, in addition to the notice provided under subsection (a) above.

10.5 Content of Notification. Notice of a Breach sent to a Covered Individual pursuant to this Article 10 will include, to the extent possible, the following:

(a) A brief description of what occurred, including the date of the Breach and the date of the discovery of the Breach, if known;

(b) A description of the types of Unsecured PHI that were involved in the Breach (for example, a Covered Individual's name, Social Security number, date of birth, home address, account number, or disability code);

(c) The steps Covered Individuals should take to protect themselves from potential harm resulting from the Breach;

(d) A brief description of the steps SDIS is taking to investigate the Breach, mitigate losses and protect against any further Breaches; and

(e) Contact procedures for Covered Individuals to ask questions or learn additional information, including a toll-free telephone number, e-mail address, Web site, or postal address.

10.6 Notice to Media Outlets. In addition to the notices provided pursuant to Section 10.1, in the event of a Breach involving more than 500 Covered Individuals of a single state or jurisdiction, SDIS will notify major print or broadcast media outlets in the geographic areas where the Covered Individuals affected by the Breach likely reside, indicating that Unsecured PHI was, or is reasonably believed to have been, accessed, acquired, or disclosed during such Breach.

10.7 Notice to HHS. For all Breaches of Unsecured PHI, SDIS will notify HHS. For a Breach involving 500 or more Covered Individuals, such notice will be provided immediately. With respect to a Breach involving fewer than 500 Covered Individuals, SDIS will maintain a log of such Breaches and annually submit the log to HHS no later than 60 days after the end of the calendar year in which such Breaches occurred.

10.8 Timeliness of Notification. Subject to Section 10.11 below, all notifications required under this Article 10 will be made without unreasonable delay, and in no case later than 60 calendar days after the discovery of a Breach by SDIS (or by the Business Associate, in the case of a notification to SDIS as required under Section 10.10).

10.9 Breaches Treated as Discovered. For purposes of this Article 10, a Breach will be treated as discovered by SDIS or Business Associate as of the first day on which such Breach is known to such entity or individual (including any person, other than the individual committing the Breach, who is a Workforce Member, or agent of SDIS or Business Associate, respectively) or by exercising reasonable diligence would have been known to the entity or individual to have occurred.

10.10 Business Associates. Each Business Associate will be contractually obligated to notify SDIS of any Breach that it discovers. Such notice will include the identification of each Covered Individual whose Unsecured PHI has been, or is reasonably believed by the Business Associate to have been, accessed, acquired, or disclosed as a result of such Breach.

10.11 Delay of Notification Authorized for Law Enforcement Purposes. If a law enforcement official determines that a notification, notice, or posting required under this Article 10 would impede a criminal investigation or cause damage to national security, such notification, notice, or posting will be delayed as provided in this Section 10.11.

(a) If the law enforcement official provides SDIS with a written statement that notification to the Covered Individual would reasonably impede the agency's activities, SDIS will suspend notification for the time period prescribed in the written statement.

(b) If a statement by a law enforcement official is made orally regarding delayed Breach notification under this Section 10.11, SDIS will:

(i) Document the statement, including the identity of the law enforcement official making the statement;

(ii) Temporarily suspend the notification procedures regarding the Covered Individual's right to notification of a Breach involving his or her Unsecured PHI; and

(iii) Limit the temporary notification suspension to no longer than 30 days from the date of the oral statement, unless during that time a written statement meeting the requirements of subsection (a) above is submitted by a law enforcement official.