

SL Goodell Insurance Services, Inc. Privacy Policies and Procedures

Table of Contents

- Management and Protection of Protected Client Data** **3**
 - 1.0 Overview:* 3
 - 2.0 Purpose:* 3
 - 3.0 Applicability:* 3
 - 4.0 Definitions:* 3
 - 5.0 Policy:* 5
 - 6.0 Enforcement:* 7
- Administrative Requirements for HIPAA Implementation** **7**
 - 1.0 Overview:* 7
 - 2.0 Purpose:* 7
 - 3.0 Applicability:* 7
 - 4.0 Special Definitions:* 7
 - 5.0 Policy:* 7
 - 6.0 Documentation Requirements:* 9
 - 7.0 Enforcement:* 9
- Minimum Necessary Provision** **9**
 - 1.0 Overview:* 9
 - 2.0 Purpose:* 10
 - 3.0 Applicability:* 10
 - 4.0 Special Definitions:* 10
 - 5.0 Policy:* 10
 - 6.0 Procedures:* 10
 - 7.0 Enforcement:* 11
- Individuals' Rights Relating to Protected Client Data** **11**
 - 1.0 Overview:* 11
 - 2.0 Purpose:* 11
 - 3.0 Applicability:* 11
 - 4.0 Special Definitions:* 12
 - 5.0 Policy:* 12
 - 6.0 Enforcement:* 14
- Business Associate Agreement** **15**
 - 1.0 Overview:* 15
 - 2.0 Purpose:* 15
 - 3.0 Applicability:* 15
 - 4.0 Special Definitions:* 15
 - 5.0 Policy:* 15
 - 6.0 Enforcement:* 16

Receipt, Use and Disclosure of Protected Client Data	16
1.0 Overview:	16
2.0 Purpose:	17
3.0 Applicability:	17
4.0 Special Definitions:	17
5.0 Policy:	17
6.0 Procedures:	19
7.0 Enforcement:	19
Complaint Process	20
1.0 Overview:	20
2.0 Purpose:	20
3.0 Applicability:	20
4.0 Special Definitions:	20
5.0 Policy:	20
6.0 Procedures:	20
7.0 Enforcement:	21
FAX Policy	22
1.0 Overview:	22
2.0 Purpose:	22
3.0 Applicability:	22
4.0 Special Definitions	22
5.0 Corporate Policies:	22
6.0 Procedure:	23
7.0 Enforcement:	23
Training Policy	23
1.0 Overview:	23
2.0 Purpose:	24
3.0 Applicability:	24
4.0 Special Definitions:	24
5.0 Policy:	24
6.0 Enforcement:	25

Management and Protection of Protected Client Data

1.0 Overview:

The Privacy Rules place certain restrictions on the acquisition, use and disclosure of Protected Healthcare Information (PHI). Further, under the rules and agreements signed by the Agency with the Health Insurance Marketplaces, and in accordance with federal regulations, the Agency must also protect Personally-Identifiable Information (PII) that we may receive, use, transmit or store about any client or prospect who may purchase health insurance coverage through the Health Insurance Marketplaces, whether federally-facilitated, state partnership or state-operated. Collectively, we will refer to PHI and PII as “Protected Client Data” and applies to the information that falls within either definition.

These policies establish the minimum care with which Protected Client Data in the custody of SL Goodell Insurance Services Inc. personnel must be accorded.

2.0 Purpose:

The purpose of this document is to provide basic instruction to all of the SL Goodell Insurance Services Inc. employees regarding the management and protection of Protected Client Data.

3.0 Applicability:

This policy applies to all SL Goodell Insurance Services Inc. employees, which is defined for the purposes of this document to be employees of all current and future subsidiaries of SL Goodell Insurance Services, Inc.

4.0 Definitions:

Covered Entity means a health plan, a health care clearinghouse, or a health care provider that transmits any health information in electronic form relating to any covered transaction.

Hybrid Entity means a single legal entity that is a covered entity whose covered functions are not its primary functions.

Protected Health Information (PHI) means individually identifiable information relating to the past, present or future physical or mental health or condition of an individual, provision of health care to an individual, or the past, present or future payment for health care provided to an individual.

Personally-Identifiable Information (PII) means any information about an individual maintained by SL Goodell Insurance Services Inc. including:

- a. Any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and
- b. Any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information

Protected Client Data means Protected Health Information and/or Personally-Identifiable Information which is used, disclosed, transmitted, or stored by SL Goodell Insurance Services Inc.

Designated Record Set means a group of records maintained by or for a covered entity, business associate or business associate subcontractor that is: the medical and billing records relating to an individual maintained by or for a health care provider; the enrollment, payment, claims adjudication, and case or medical management systems maintained by or for a health plan, or; used, in whole or in part, by or for a covered entity to make decisions about individuals.

Treatment, Payment and Health Care Operations (TPO) includes all of the following:

- a. *Treatment* means the provision, coordination, or management of health care and related services, consultation between providers relating to an individual, or referral of an individual to another provider for health care.
- b. *Payment* means activities undertaken to obtain or provide reimbursement for health care, including determinations of eligibility or coverage, billing, collections activities, medical necessity determinations and utilization review.
- c. *Health Care Operations* includes functions such as quality assessment and improvement activities, reviewing competence or qualifications of health care professionals, conducting or arranging for medical review, legal services and auditing functions, business planning and development, and general business and administrative activities including the creation of de-identified health information as defined by these regulations.

Disclosure means the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

Use means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

Personal Representative means a person who has authority under applicable law to make decisions related to health care on behalf of an adult or an emancipated minor, or the parent,

guardian, or other person who is authorized under law to make health care decisions on behalf of an un-emancipated minor.

Employees means all employees of SL Goodell Insurance Services Inc. as well as its temporary employees, interns, independent contractors, trainees, and other persons whose conduct, in the performance of work for the SL Goodell Insurance Services Inc. its offices, programs or facilities.

Privacy Rules means the rules adopted by various state and federal agencies to implement the requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and regulations promulgated under this Act as well as those obligations that arise under the privacy and security standards adopted by the Health Insurance Marketplaces, pursuant to 45 C.F.R. §155.260.

5.0 Policy:

For details on specific requirements, refer to the appropriate policies in this manual as indicated in brackets.

- A. Generally: Protected Client Data shall not be obtained, used or disclosed except as permitted or required by law.

- B. Permitted and Required Uses and Disclosures: Protected Client Data may or shall be disclosed as follows:
 - 1. To the individual [\[Individuals' Rights Related to Protected Client Data\]](#). (Page 12)
 - 2. To carry out TPO activities as allowed under HIPAA and/or pursuant to and in compliance with a current and valid Authorization [\[Receipt, Use and Disclosure of Protected Client Data\]](#). (Page 18)
 - 3. In keeping with a Business Associate Subcontractor agreement [\[Business Associate Agreement\]](#). (Page 16)
 - 4. As otherwise allowed or required under the HIPAA Rules or other federal and/or state laws concerning privacy of information that is used by Agency in the course of its business operations.

- C. Minimum Necessary: Generally, when obtaining, using or disclosing Protected Client Data, or when requesting Protected Client Data from another entity, reasonable efforts must be made to limit the Protected Client Data used or disclosed to the minimum necessary to accomplish the intended purpose. However, the Privacy rules were not intended to severely complicate business processes and SL Goodell Insurance Services Inc. may, where appropriate, use a single format to provide data containing Protected Client Data for our various services [\[Minimum Necessary Provision\]](#). (Page 10)

- D. Accounting for Disclosures: An individual has a right to an accounting of disclosures of his/her Protected Client Data for up to a six-year period [\[Right to an Accounting for Disclosures\]](#). (Page 15)

- E. De-identified Protected Client Data: Protected Client Data may be considered not to be individually identifiable in the following circumstances:
1. A person with appropriate knowledge and experience with generally acceptable statistical and scientific principles and methods determines that the risk is very small that the information could be used, alone or with other reasonably available information, to identify the individual who is the subject of the information (**Generally, SL Goodell Insurance Services Inc. will not use this approach to de-identification.**)
 2. The following identifiers of the individual (and relatives, employers or household members) are removed (**This is the “Safe Harbor” method that SL Goodell Insurance Services Inc. will generally use**):
 - Names
 - Information relating to the individual's geographic subdivision if it contains fewer than 20,000 people
 - Elements of dates (except year) directly related to the individual
 - All ages and elements of dates that indicate age for individuals over 89, unless aggregated into a single category of age 90 and older
 - Telephone numbers
 - Fax numbers
 - Email addresses
 - Social security numbers
 - Medical record numbers
 - Health plan beneficiary numbers
 - Account numbers
 - Certificate or 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; full face photographic images
 - Any other unique identifying number, characteristic or code.
 3. As allowed in the Privacy Rules, SL Goodell Insurance Services Inc. shall provide a number of longitudinal identifiers in the de-identified data. These identifiers shall not allow identification of the individual who is the subject of this data in that:
 - a. These identifiers will be encrypted using industry level encryption techniques
 - b. The method of encryption shall not be divulged to the received of the de-identified data
- F. Complaint Process: SL Goodell Insurance Services Inc. must put into place a process for individuals to make complaints about our Privacy policies and procedures and/or our compliance with those policies and procedures [[Complaint Processes](#)]. (Page 20)
- G. Documentation: Every employee must maintain written or electronic copies of all policies and procedures, communications, actions, activities or designations as are required to be documented under this manual for a period of six (6) years from the later of the date of creation or the last effective date. **NOTE: This is the documentation requirement**

under HIPAA and does not negate longer retention periods that are mandated under other existing state or federal laws or regulations.

6.0 Enforcement:

An employee found to have violated this policy shall be subject to disciplinary action, up to and including termination of employment. In the case where inappropriate access, use or disclosure of Protected Client Data was or may have been involved, such individuals may additionally be reported to the appropriate enforcement agencies.

Administrative Requirements for HIPAA Implementation

1.0 Overview:

The Privacy Rules require that a Business Associate have in place appropriate administrative safeguards to protect the privacy of Protected Client Data.

2.0 Purpose:

To provide instructions regarding SL Goodell Insurance Services Inc.'s obligations relating to the implementation of administrative requirements of the Privacy Rules.

3.0 Applicability:

This policy applies to all SL Goodell Insurance Services Inc. employees, which is defined for the purposes of this document to be employees of all current and future subsidiaries of SL Goodell Insurance Services Inc.

4.0 Special Definitions:

Privacy Notice means the notice of privacy practices relating to an entity's use and disclosure of Protected Client Data that is mandated under Privacy Rules for distribution to all individuals whose information will be collected by or on behalf of the entity.

5.0 Policy:

- A. **Personnel Designations:** SL Goodell Insurance Services Inc. shall designate and document designations of the following:
 1. **Privacy Officer:** SL Goodell Insurance Services Inc. shall designate an individual as the Privacy Officer, responsible for the development and implementation of corporate-wide policies and procedures relating to the safeguarding of Protected Client Data.
 2. **Contact Person or Office:** SL Goodell Insurance Services Inc. shall designate an individual, position title, or office that will be responsible for receiving complaints relating to Protected Client Data and for providing information about the agency's privacy practices.
 3. **Persons with access to Protected Client Data** will be listed by title and each department shall include a listing of individual's names with our Privacy Officer

and update on a periodic basis retaining the previous listing for a period of not less than 6 years.

- B. Training Requirements: SL Goodell Insurance Services Inc. shall document the following training actions:
1. All SL Goodell Insurance Services Inc. employees shall receive training on applicable policies and procedures relating to Protected Client Data as necessary and appropriate for such persons to carry out their functions within the SL Goodell Insurance Services Inc.
 2. Each new employee shall receive the training as described above within a reasonable time after joining SL Goodell Insurance Services Inc.
 3. Each employee whose functions are impacted by a material change in the policies and procedures relating to Protected Client Data, or by a change in position or job description, shall receive the training as described above within a reasonable time after the change becomes effective.
- C. Safeguards: SL Goodell Insurance Services Inc. shall have in place appropriate administrative, technical, and physical safeguards to reasonably safeguard Protected Client Data from intentional or unintentional unauthorized receipt, use or disclosure.
- D. Complaint Process: SL Goodell Insurance Services Inc. shall have in place a process for individuals to make complaints about SL Goodell Insurance Services Inc.'s HIPAA policies and procedures and/or SL Goodell Insurance Services Inc.'s compliance with those policies and procedures, and shall document all complaints received and the disposition of each complaint.
- E. Sanctions: SL Goodell Insurance Services Inc. shall have in place, apply and document application of appropriate sanctions against employees who fail to comply with HIPAA policies and procedures. (Note - there are exceptions for disclosures made by employees who qualify as whistleblowers or certain crime victims.)
- F. Mitigation Efforts Required: SL Goodell Insurance Services Inc. to the extent practicable, shall mitigate any harmful effects of unauthorized uses or disclosures of Protected Client Data by SL Goodell Insurance Services Inc. or any of its Business Associates.
- G. Prohibition on Intimidating or Retaliatory Acts: Neither SL Goodell Insurance Services Inc. nor any employee shall intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise of their rights or participation in any process relating to HIPAA compliance, or against any person for filing a complaint with the Secretary of the U.S. Department of Health and Human Services, participating in an investigation, compliance review, proceeding or hearing, or engaging in reasonable opposition to any act or practice that the person in good faith

believes to be unlawful under the Privacy Rules as long as the action does not involve disclosure of Protected Client Data in violation of the regulations.

- H. **Policies and Procedures:** SL Goodell Insurance Services Inc. shall document the following actions relating to its policies and procedures:
1. **Required Policies and Procedures:** SL Goodell Insurance Services Inc. shall design and implement policies and procedures to assure appropriate safeguarding of Protected Client Data in its operations.
 2. **Changes to Policies and Procedures:** SL Goodell Insurance Services Inc. shall change its policies and procedures as necessary and appropriate to conform to changes in law or regulation. SL Goodell Insurance Services Inc. may also make changes to policies and procedures at other times as long as the policies and procedures are still in compliance with applicable law. Where necessary, SL Goodell Insurance Services Inc. shall make correlative changes in its Privacy Notice.

6.0 Documentation Requirements:

SL Goodell Insurance Services Inc. must maintain the required policies and procedures in written or electronic form, and must maintain written or electronic copies of all communications, actions, activities or designations as are required to be documented hereunder, or otherwise under the Privacy Rules, for a period of six (6) years from the later of the date of creation or the last effective date.

7.0 Enforcement:

Any employee found to have violated this policy shall be subject to disciplinary action, up to and including termination of employment. In the case where inappropriate access, use or disclosure of Protected Client Data was or may have been involved, such individuals may additionally be reported to the appropriate enforcement agencies.

Minimum Necessary Provision

1.0 Overview:

The Privacy Rules place certain restrictions on the receipt, use and disclosure of Protected Client Data in regards to the amount reasonably necessary to accomplish the task being performed. However, the Privacy Rules also allow Protected Client Data to be disclosed for business appropriate needs.

The policies developed by SL Goodell Insurance Services Inc. will follow this business appropriate philosophy as well as that of administrative simplification, which is the subsection of the HIPAA law under which the Privacy Rule was developed. SL Goodell Insurance Services Inc. shall use standard data formats for information acquisition or disclosure and tailor these formats to contain a business reasonable minimum necessary amount of Protected Client Data. The SL Goodell Insurance Services Inc. policies establish the minimum necessary use

provisions for Protected Client Data in the custody of SL Goodell Insurance Services Inc. employees.

2.0 Purpose:

To issue instructions regarding the SL Goodell Insurance Services Inc. obligations relating to the Privacy Rules to obtain, use and disclose only the minimum amount of Protected Client Data (Protected Client Data) necessary to accomplish the intended purpose.

3.0 Applicability:

This policy applies to all SL Goodell Insurance Services Inc. employees, which is defined for the purposes of this document to be employees of all current and future subsidiaries of SL Goodell Insurance Services Inc.

4.0 Special Definitions:

None

5.0 Policy:

SL Goodell Insurance Services Inc. will make reasonable efforts to ensure that the minimum necessary amount of Protected Client Data is disclosed, used, or requested to accomplish the intended purpose. Exceptions to the minimum necessary requirement include disclosures:

- A. To the individual who is the subject of the information.
- B. Made pursuant to an authorization provided by the individual.
- C. To healthcare providers for treatment purposes.
- D. Required for compliance with the standardized HIPAA transactions.
- E. Made to the Secretary of HHS of his agent pursuant to a privacy investigation.
- F. Otherwise required by the Privacy Rules or other law.

Employees will be trained on the policy and procedures developed to apply these principles to the use or disclosure of, or requests for Protected Client Data.

6.0 Procedures:

The following procedures will be implemented to ensure that this policy is enforced effectively across all parts of [Agency].

- A. Each user of a system which accesses Protected Client Data shall be identified and the classes or types of Protected Client Data to which access is needed and any conditions appropriate to such access will be established. It will be the responsibility of the Privacy Officer to maintain this information as outlined in the Access to Systems Containing Protected Client Data procedures [\[Access to Systems Containing Protected Client Data\]](#).
- B. Reasonable efforts will be taken to limit the access of each user of Protected Client Data to the amount needed to carry out the individual's duties. These efforts will include internal use of Protected Client Data.
- C. For situations where Protected Client Data disclosure occurs on a routine and recurring basis, the Protected Client Data disclosed will be limited to the amount of information reasonably necessary to achieve the purpose of the disclosure.
- D. Requests for disclosures that are not routine and recurring and thereby covered by SL Goodell Insurance Services Inc. standard procedures (other than to the individual, the Secretary of HHS or his agent or where required by law) shall be reviewed by the Privacy Officer to determine that the minimum necessary provision is applied to the extent reasonable.
- E. Questions regarding these procedures should be directed to the SL Goodell Insurance Services Inc. Privacy Officer.

7.0 Enforcement:

An employee found to have violated this policy shall be subject to disciplinary action, up to and including termination of employment. In the case where inappropriate access, use or disclosure of Protected Client Data was or may have been involved, such individuals may additionally be reported to the appropriate enforcement agencies.

Individuals' Rights Relating to Protected Client Data

1.0 Overview:

The Privacy Rules provide individuals with certain rights regarding their Protected Client Data.

2.0 Purpose:

It is the purpose of this section to provide instructions regarding SL Goodell Insurance Services Inc.'s obligations in complying with an individual's rights under the Privacy Rules to provide the individual with access to, a copy of and an accounting for disclosures of Protected Client Data (Protected Client Data) relating to the individual.

3.0 Applicability:

This policy applies to all SL Goodell Insurance Services Inc. employees, which is defined for the purposes of this document to be employees of all current and future subsidiaries of SL Goodell Insurance Services Inc.

4.0 Special Definitions:

Personal Representative means a person who has authority under applicable law to make decisions related to health care on behalf of an adult or an emancipated minor, or the parent, guardian, or other person who is authorized under law to make health care decisions on behalf of an un-emancipated minor.

5.0 Policy:

1. RIGHT TO ACCESS AND COPY PROTECTED CLIENT DATA: Individuals have a right to access and copy their Protected Client Data and any information in designated record sets except as follows:

- A. Provision of Access: SL Goodell Insurance Services Inc. must provide an individual with access to the information in the form or format requested if it is readily producible in such form or format, or in a readable hard copy or other form or format as mutually agreed to, either by arranging for a convenient time and place for inspection and copying, or mailing the information at the individual's request.
 - 1. If the information is maintained in more than one place, the information need only be produced once in response to a current request for access.
 - 2. SL Goodell Insurance Services Inc. may provide a summary of the information in lieu of providing access, or may provide an explanation of the information to which access is provided if the individual, in advance, agrees.
 - 3. SL Goodell Insurance Services Inc. may impose a reasonable, cost-based fee for copying, or preparing a summary or explanation of the information provided that the fee includes only the cost of copying supplies, postage, and labor for preparing the summary or explanation as agreed to by the individual.

- B. Denial of Access: SL Goodell Insurance Services Inc. must provide a timely, written denial of access to the individual, written in plain language, explaining the basis for the denial, any applicable right of review, and describe how the individual may complain to SL Goodell Insurance Services Inc. (including name or title of contact, and phone number) or the U.S. Secretary of Health and Human Services.
 - 1. To the extent possible, the individual must be given access to any information requested after excluding the information for which entity has grounds for denying access.
 - 2. If SL Goodell Insurance Services Inc. does not maintain the information for which access has been requested, but knows where it is maintained, SL Goodell Insurance Services Inc. must inform the individual where to direct the request for access.

- C. Denial of Access without a right of review: Individuals may be denied access and right to copy Protected Client Data relating to the individual when:
 - 1. Information was compiled in anticipation of litigation.
 - 2. Care was provided under the direction of a correctional institution and provision of access would jeopardize health, safety, or rehabilitation.
 - 3. Information was collected in the course of research that includes treatment of the individual and the individual agreed to a suspension of the right of access during the research period.
 - 4. Where such access would provide the individual access to the Protected Client Data of other individuals.

- D. Documentation: SL Goodell Insurance Services Inc. must document and retain for six years from the date of its creation the designated record sets subject to access and the names or titles of persons responsible for receiving and processing requests for access.

2. RIGHT TO REQUEST AN AMENDMENT OF PROTECTED CLIENT DATA: An individual has the right to have SL Goodell Insurance Services Inc. amend Protected Client Data or other information in the designated record set for as long as SL Goodell Insurance Services Inc. maintains the information. SL Goodell Insurance Services Inc. must act on the request within sixty (60) days of receipt, or within ninety (90) days if SL Goodell Insurance Services Inc. notifies the individual within the first 60 days of the reasons for delay and the date by which action will be taken.

A. Accepting the Amendment: If SL Goodell Insurance Services Inc. accepts the amendment, in whole or in part, it must:

1. Make the amendment by, at minimum, identifying the affected records and appending or otherwise providing a link to the location of the amendment.
2. Timely inform the individual that the amendment is accepted, and obtain his/her identification of and agreement to have SL Goodell Insurance Services Inc. notify relevant persons with a need to know.
3. Make reasonable efforts to inform and timely provide the amendment to those persons and others, including Business Associates, that SL Goodell Insurance Services Inc. knows to have the affected Protected Client Data and that may have relied, or be foreseen to rely, on that information to the detriment of the individual.

B. Denying the Amendment: SL Goodell Insurance Services Inc. may deny the request if it determines that the record:

1. Was not created by SL Goodell Insurance Services Inc. (unless the individual provides reasonable basis to believe that the originator of the records is no longer available to act on the request);
2. Is not part of the designated record set;
2. Would not be available for inspection; or
3. Is accurate and complete.

C. Denial Requirements: If SL Goodell Insurance Services Inc. denies the amendment, in whole or part, it must:

1. Provide the individual with a timely denial, written in plain language and including:
 - a. The basis for denial;
 - b. Notice of the individual's right to submit a written statement of disagreement, and instructions on how to file the statement, or to request that future disclosures of the Protected Client Data include copies of the request and the denial; and
 - c. A description of how the individual may complain about the decision to SL Goodell Insurance Services Inc. or to the U. S. Secretary of Health and Human Services.

2. Permit the individual to submit a statement of disagreement (but entity may reasonably limit its length).
3. Provide a copy of any rebuttal prepared to the individual.
4. As appropriate, identify the part of the record subject to the disputed amendment and append or otherwise link the request, the denial, and any statement of disagreement or rebuttal to the record.
5. For future disclosures of the record, include any statement of disagreement or, in response to the individual's request, the amendment request and the denial (or an accurate summary of either of the foregoing). If standard transaction format does not permit the appending of the additional information, it must be transmitted separately to the recipient of the standard transaction.

D. Notification of Amendment: If SL Goodell Insurance Services Inc. is informed by a covered entity or another business associate of a covered entity about an amendment to the record, SL Goodell Insurance Services Inc. must amend the information in its record by, at a minimum, identifying the affected records and appending or otherwise providing a link to the location of the amendment.

E. Documentation: SL Goodell Insurance Services Inc. must document the titles of the persons or offices responsible for receiving and processing requests for amendments.

3. RIGHT TO AN ACCOUNTING OF DISCLOSURES: An individual has a right to receive an accounting of disclosures of their Protected Client Data for the previous six years. Disclosures excepted from this accounting requirement:

- A. To carry out treatment, payment and health care operations.
- B. To individuals or groups of individuals allowed under an authorization signed by the individual who is the subject of the Protected Client Data.
- C. To the individual to whom the Protected Client Data relates.
- D. For national security or intelligence purposes as defined in the privacy regulations.
- E. To correctional institutions or law enforcement officials.
- F. That occurred prior to the compliance date for the covered entity.
- G. The Agency must temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official, as provided, for the time specified by such agency or official if requested in accordance with these provisions.

6.0 Enforcement:

An employee found to have violated this policy shall be subject to disciplinary action, up to and including termination of employment. In the case where inappropriate access, use or disclosure of Protected Client Data was or may have been involved, such individuals may additionally be reported to the appropriate enforcement agencies.

Business Associate Agreement

1.0 Overview:

The Privacy Rules impose certain requirements on Business Associates who create, receive, use or disclose Protected Client Data on behalf of their covered entity partners. SL Goodell Insurance Services Inc. must comply with the requirements in this section.

2.0 Purpose:

To provide instructions to all SL Goodell Insurance Services Inc. employees regarding the necessity of and the requirements for Business Associate agreements (including in some cases other covered entities) relating to Business Associate's who receive, use or disclosure Protected Client Data on behalf of SL Goodell Insurance Services Inc.

3.0 Applicability:

This policy applies to all SL Goodell Insurance Services Inc. employees, which is defined for the purposes of this document to be employees of all current and future subsidiaries of SL Goodell Insurance Services Inc.

4.0 Special Definitions:

None

5.0 Policy:

- A. Generally: SL Goodell Insurance Services Inc. may disclose Protected Client Data to a Business Associate Subcontractor, or allow a Business Associate Subcontractor to create or receive Protected Client Data on SL Goodell Insurance Services Inc. behalf, if adequate assurances that the Business Associate Subcontractor will appropriately safeguard the Protected Client Data are obtained by SL Goodell Insurance Services Inc. SL Goodell Insurance Services Inc. must document these assurances through a written agreement. This requirement does not apply with respect to:
 - 1. Disclosures made to a provider concerning the individual's treatment, payment or health care operations, or;
 - 2. Uses or disclosures made to a governmental agency for purposes of public benefit eligibility or enrollment determinations where such agency is authorized by law to make these determinations.

- B. Content Requirements: The agreement between SL Goodell Insurance Services Inc. and a Business Associate Subcontractor must meet the following requirements, as applicable:
 - 1. Establish permitted and required uses or disclosures of Protected Client Data that are consistent with those authorized for the entity, except that the agreement may permit the Business Associate Subcontractor to use or disclose Protected Client Data for its own management and administration if such use or disclosure is required by law or the Business Associate Subcontractor obtains reasonable assurance from the entity to which the Protected Client Data is disclosed that the confidentiality of the Protected Client Data will be maintained.
 - 2. Provide that the Business Associate Subcontractor will:

- i. Not use or disclose the Protected Client Data except as authorized under the agreement or required by law.
- ii. Use safeguards to prevent unauthorized use or disclosure.
- iii. Report unauthorized uses or disclosures to the covered entity.
- iv. Pass on the same obligations relating to protection of Protected Client Data to any subcontractors or agents.
- v. Make Protected Client Data available for access by the individual or his/her personal representative, in accordance with relevant law and policy.
- vi. Make Protected Client Data available for amendment, and incorporate any approved amendments to Protected Client Data, in accordance with relevant law and policy.
- vii. Make information available for the provision of an accounting of uses and disclosures in accordance with relevant law and policy.
- viii. Make its internal practices, books and records relating to its receipt or creation of Protected Client Data available to the Secretary of HHS for purposes of determining the entity's compliance with Privacy Rules.
- ix. If feasible, return or destroy all Protected Client Data upon termination of contract; if any Protected Client Data is retained, continue to extend the full protections specified herein as long as the Protected Client Data is maintained.
- x. Authorize termination of the agreement by the entity upon a material breach by the Business Associate Subcontractor.

C. Compliance Responsibilities: If SL Goodell Insurance Services Inc. knows of a pattern or practice of the Business Associate Subcontractor that amounts to a material violation of the agreement, SL Goodell Insurance Services Inc. must attempt to cure the breach to end the violation, and if unsuccessful, terminate the agreement. If terminating the agreement is not feasible SL Goodell Insurance Services Inc. must report the problem to the Secretary of HHS.

6.0 Enforcement:

An employee found to have violated this policy shall be subject to disciplinary action, up to and including termination of employment. In the case where inappropriate access or use of Protected Client Data was or may have been involved, these individuals may additionally be reported to the appropriate law enforcement agencies.

Receipt, Use and Disclosure of Protected Client Data

1.0 Overview:

The Privacy Rules impose certain requirements on covered entities and Business Associates who create, receive, use or disclose Protected Client Data on behalf of their covered entity partners.

2.0 Purpose:

To provide instructions to all SL Goodell Insurance Services Inc. employees regarding the receipt, uses and disclosures of Protected Client Data, which are permitted or required by HIPAA.

3.0 Applicability:

This policy applies to all SL Goodell Insurance Services Inc. employees, which is defined for the purposes of this document to be employees of all current and future subsidiaries of SL Goodell Insurance Services Inc.

4.0 Special Definitions:

Public Health Authority means a governmental agency or authority, or a person or entity acting under a grant of authority from or a contract with such a public agency, including the employees or agents of the public agency, its contractors and those to whom it has granted authority, that is responsible for public health matters as part of its official mandate.

5.0 Policy:

State and federal law permit and require certain receipt, uses and disclosures of Protected Client Data such as those related to Business Associate Agreements. Additional uses and/or disclosures are allowed or required that related to public responsibility that require no agreement or authorization on the part of the individual who is the subject of the Protected Client Data. It is the policy of SL Goodell Insurance Services Inc. to obtain, use and disclose Protected Client Data only as permitted and/or required by law or regulation including the following situations:

- A. Treatment, Payment or Healthcare Operations: Protected Client Data may be used or disclosed for the purposes of providing treatment, payment or healthcare operations. Such disclosures will be made only as allowed by and pursuant to prevailing state and federal law.
 - 1. Discussions involving Protected Client Data shall be conducted only in appropriate business areas including but not limited to offices, conference rooms and other non-public areas;
 - 2. Conducted only for the purpose of fulfilling a legitimate business need; and
 - 3. Conducted with regard to and in compliance with the “minimum necessary provision,” [\[Minimum Necessary Provision\]](#). (Page 10)

- B. Contained in a Business Associate Agreement: For permitted and required uses or disclosures of Protected Client Data that are consistent with those authorized by the covered entity in a Business Associate agreement.

- C. Required by Law: Protected Client Data may be used or disclosed to the extent such use or disclosure complies with and is limited to the requirements of such law.
 - 1. Abuse and Neglect: Except for reports of child abuse or neglect, Protected Client Data about an individual believed to be a victim of abuse, neglect, or domestic violence may be disclosed to a governmental authority authorized to receive such reports if the individual agrees or the reporting entity believes, in the exercise of professional judgment, that the disclosure is necessary to prevent

serious physical harm. If the individual lacks the capacity to agree, disclosure may be made if not intended for use against the individual and delaying disclosure would materially hinder law enforcement activity. The individual whose Protected Client Data has been released must be promptly informed that the report was made unless doing so would place the individual at risk of serious harm.

2. Judicial Proceedings: Protected Client Data may be disclosed in response to a court order.
3. Law Enforcement: Protected Client Data may be disclosed for the following law enforcement purposes and under the specified conditions:
 - i. Pursuant to court order or as otherwise required by law, i.e. laws requiring the reporting of certain types of wounds or injuries;
 - ii. Decedent's Protected Client Data may be disclosed to alert law enforcement to the death if entity suspects that death resulted from criminal conduct;

D. Serious Threats to Health or Safety: Consistent with applicable law and ethical standards, Protected Client Data may be used or disclosed if the entity believes in good faith that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to a person or the public, and disclosure is to someone reasonably able to prevent or lessen the threat, or the disclosure is to law enforcement authorities to identify or apprehend an individual who has admitted to violent criminal activity that likely caused serious harm to the victim or who appears to have escaped from lawful custody. Disclosures of admitted participation in a violent crime are limited to the individual's statement of participation and are not permitted when the information is learned in the course of treatment to affect the propensity to commit the subject crime, or through counseling, or therapy or a request to initiate the same.

E. Specialized Government Functions:

1. National Security and Intelligence: Protected Client Data may be disclosed to authorized federal officials for the conduct of lawful intelligence, counter intelligence, and other activities authorized by the National Security Act.
2. Protective services: Protected Client Data may be disclosed to authorized federal officials for the provision of protective services to the President, foreign heads of state, and others designated by law, and for the conduct of criminal investigations of threats against such persons.
3. Public Benefits: Protected Client Data relevant to administration of a government program providing public benefits may be disclosed to another governmental program providing public benefits serving the same or similar populations as necessary to coordinate program functions or improve administration and management of program functions.

F. Workers' Compensation: Protected Client Data may be disclosed as authorized and to the extent necessary to comply with laws relating to workers' compensation and other similar programs.

6.0 Procedures:

The following procedures will be implemented to ensure that this policy is enforced effectively across all parts of SL Goodell Insurance Services Inc.

- A. Any request for disclosure of Protected Client Data pursuant to a court order, warrant or subpoena must be directed to the appropriate corporate individual for review and action. Upon receipt of such court order, warrant or subpoena, Employees shall include an acknowledgement receipt to insure that the document was actually received by the appropriate corporate individual and will retain a copy of the court order, warrant or subpoena received. If the acknowledgement is not received within two working days of submitting to the appropriate corporate individual, then the request will be resubmitted to the Privacy Officer.
- B. Any request for disclosure of Protected Client Data by a law enforcement agent must be directed to the appropriate corporate individual for review and action. Any such requests shall include an acknowledgement of receipt to insure that the request was actually received by the appropriate corporate individual and will retain a copy of the request received. If the acknowledgement is not received within two working days of submitting to the appropriate corporate individual, then the request will be resubmitted to the Privacy Officer.
- C. Any request for disclosure of Protected Client Data by a public health authority must be directed to the appropriate corporate individual for review and action. Any such request will include an acknowledgement of receipt to insure that the document was actually received by the appropriate corporate individual and will retain a copy of the request. If the acknowledgement is not received within two working days of submitting to the appropriate corporate individual, then the request will be resubmitted to the Privacy Officer.
- D. Any request for disclosure of Protected Client Data by a national security, intelligence or other federal agency must be directed to the appropriate corporate individual for review and action. Any such request will include an acknowledgement of receipt to insure that the document was actually received by the appropriate corporate individual and will retain a copy of the request. If the acknowledgement is not received within two working days of submitting to the appropriate corporate individual, then the request will be resubmitted to the Privacy Officer.

7.0 Enforcement:

An employee found to have violated this policy shall be subject to disciplinary action, up to and including termination of employment. In the case where inappropriate access, use or disclosure of Protected Client Data was or may have been involved, such individuals may additionally be reported to the appropriate enforcement agencies.

Complaint Process

1.0 Overview:

The Privacy Rules require that SL Goodell Insurance Services Inc. provide a process for individuals to make complaints concerning the SL Goodell Insurance Services Inc.'s policies and procedures required by these regulations and document all complaints received, and the dispositions of these complaints, if any.

2.0 Purpose:

To issue instructions regarding the SL Goodell Insurance Services Inc. obligations relating to the Privacy Rules to provide a process for individuals to complain about the entity's policies and procedures and the requirement to document complaints received and the disposition of these complaints.

3.0 Applicability:

This policy applies to all SL Goodell Insurance Services Inc. employees, which is defined for the purposes of this document to be employees of all current and future subsidiaries of SL Goodell Insurance Services Inc.

4.0 Special Definitions:

None

5.0 Policy:

SL Goodell Insurance Services Inc. shall maintain a process to receive complaints from individuals about the SL Goodell Insurance Services Inc. privacy policies and procedures, for complaints from individuals who believe their privacy rights have been violated and from employees or Business Associate who believe that SL Goodell Insurance Services Inc. is not abiding by its policies and procedures and/or assurances concerning Protected Client Data. This process shall include the following:

- A. A designated person to provide information about submitting a complaint whose name or title and telephone number will be published to the individuals, employees and Business Associates.
- B. A system and software with which to record complaints received by the named individual and the dispositions of complaints recorded, if any.
- C. SL Goodell Insurance Services Inc. shall work in good faith to resolve complaints received to the satisfaction of the submitter, where possible.

6.0 Procedures:

The following procedures will be implemented to ensure that this policy is enforced effectively across all parts of SL Goodell Insurance Services Inc.

- A. Complaints shall be submitted in writing on paper or electronically.
- B. Complaints shall be entered into the complaint tracking system either automatically or by the individual designated to provide information on the SL Goodell Insurance Services

Inc. complaint process and when manually entered shall be in the exact words provided by the submitter.

- C. The SL Goodell Insurance Services Inc. Privacy Officer shall investigate complaints and make a determination as to whether or not the complaint has merit.
- D. The SL Goodell Insurance Services Inc. Privacy Officer shall present complaints received to the SL Goodell Insurance Services Inc. Privacy Committee at the next scheduled meeting of the committee.
- E. If the Privacy Officer has completed the investigation of the complaint and made a determination, such determination shall be presented to the SL Goodell Insurance Services Inc. Privacy Committee.
- F. If the investigation has not been completed nor a provisional determination made by the Privacy Officer, it shall be the prerogative of the Privacy Committee to make a summary determination or to direct the Privacy Officer to continue with the investigation and to report on the complaint at the next scheduled meeting.
- G. If a determination is made that SL Goodell Insurance Services Inc. is in violation of the privacy provisions of the Privacy Rules or that changes are needed in the Notice of Privacy Practices or Business Associate agreement to clarify the allowed practices of SL Goodell Insurance Services Inc. the SL Goodell Insurance Services Inc. Privacy Committee shall determine the actions that SL Goodell Insurance Services Inc. shall take.
- H. Complaint determinations and actions that SL Goodell Insurance Services Inc. takes pursuant to such complaints, if any, shall be reported to the submitter of the complaint, if such person is known.
- I. The SL Goodell Insurance Services Inc. Privacy Officer, or his designated agent, shall update the complaint tracking system with the findings of the Privacy Officer's investigation, any determination made, direction or actions of the SL Goodell Insurance Services Inc. Privacy Committee with regard to the complaint and a copy of any information provided to the submitter in response to their complaint.

7.0 Enforcement:

Any employee found to have violated this policy shall be subject to disciplinary action, up to and including termination of employment. In the case where inappropriate access, use or disclosure of Protected Client Data was or may have been involved, such individuals may additionally be reported to the appropriate enforcement agencies.

FAX Policy

1.0 Overview:

The Privacy Rules require that SL Goodell Insurance Services Inc. implement appropriate administrative, technical, and physical safeguards to protect the privacy of Protected Client Data.

2.0 Purpose:

To provide instructions to all SL Goodell Insurance Services Inc. employees regarding to the use of fax with respect to Protected Client Data and the measures necessary to maintain an adequate level of security from such information. This policy defines rules necessary to achieve this level of protection. These standards are designed to minimize the potential exposure to SL Goodell Insurance Services Inc. from damages, which may result from unauthorized disclosure of Protected Client Data through facsimile use.

3.0 Applicability:

This policy applies to all SL Goodell Insurance Services Inc. employees, which is defined for the purposes of this document to be employees of all current and future subsidiaries of SL Goodell Insurance Services Inc.

4.0 Special Definitions

FAX: An electronic facsimile of a document stored as a series of zeros and ones (binary data) that can be transmitted like normal computer data. When received by a fax machine the incoming stream of is translated into dots creating a representation of the original document.

Inappropriate Disclosure: The intentional or unintentional revealing of Protected Client Data to people who do not have a need to know such information.

5.0 Corporate Policies:

Employees must exercise utmost caution when sending faxes to parties outside of SL Goodell Insurance Services Inc. Faxes containing Protected Client Data should only be received on and sent to user or departmental specific fax machines and not to systems that have general access.

In cases where Protected Client Data is received from outside on a non-departmental specific fax machine the receiving department shall notify the SL Goodell Insurance Services Inc. Privacy Officer of the source of such information. The employee shall communicate the approved fax number to the external entity and record such actions. Should Protected Client Data be disclosed by fax to an inappropriate party, SL Goodell Insurance Services Inc. shall, to the extent possible, remediate such disclosures.

All fax documents sent by SL Goodell Insurance Services Inc. employees shall contain the following statement:

THIS FAX IS INTENDED FOR THE INDIVIDUAL/INDIVIDUALS OR ENTITY/ENTITIES NAMED ABOVE AND MAY BE COVERED BY COPYRIGHTS, BUSINESS PARTNER CONFIDENTIALITY AGREEMENTS, NONDISCLOSURES OR OTHER LEGALLY BINDING INSTRUMENTS. IF YOU ARE NOT THE INTENDED RECIPIENT, DO NOT READ, COPY, USE OR DISCLOSE THE CONTENTS OF THIS COMMUNICATION TO OTHERS. IMMEDIATELY NOTIFY THE SENDER BY REPLY FAX, DESTROY ALL HARD COPIES AND DELETE THIS DOCUMENT FROM ALL SYSTEMS. THANK YOU!

6.0 Procedure:

In the case where data that contains Protected Client Data is disclosed by fax machine use to an inappropriate party, the following procedure shall be followed:

- A. The receiving party shall be contacted by telephone at the earliest opportunity and requested to destroy the fax without reading.
- B. The name of the company, the person contacted, the date and time shall be recorded as well as any comments made by the person receiving such calls.
- C. A fax shall also be sent to the receiving party containing the same instructions as detailed for the phone call requesting a return fax message indicating that the requested action was taken.
- D. The cause of the inappropriate disclosure shall be determined and reported to the SL Goodell Insurance Services Inc. Privacy Officer.
- E. Methods to prevent a re-occurrence of the inappropriate disclosure shall be formulated and put into place.
- F. Any additional actions prescribed by regulations shall be performed to the extent possible.

7.0 Enforcement:

Any employee found to have violated this policy shall be subject to disciplinary action, up to and including termination of employment. In the case where inappropriate access, use or disclosure of Protected Client Data was or may have been involved, such individuals may additionally be reported to the appropriate enforcement agencies.

Training Policy

1.0 Overview:

The Privacy Rules require that SL Goodell Insurance Services Inc. train their employees on the requirements of our Privacy policies and procedures developed to protect the Protected Client

Data to which employees are provided access. The SL Goodell Insurance Services Inc. has determined that all employees of SL Goodell Insurance Services Inc. shall be trained on Privacy so that we can provide the necessary assurances for the protection of Protected Client Data to our clients, vendors and business partners as required under the Privacy Rules.

2.0 Purpose:

To provide instructions to all SL Goodell Insurance Services Inc. employees regarding the requirement for HIPAA training.

3.0 Applicability:

This policy applies to all SL Goodell Insurance Services Inc. employees, which is defined for the purposes of this document to be employees of all current and future subsidiaries of SL Goodell Insurance Services Inc.

4.0 Special Definitions:

None

5.0 Policy:

General: It is the policy of SL Goodell Insurance Services Inc. that all employees of SL Goodell Insurance Services Inc. and its current and future subsidiaries be trained on Privacy and the corporate policies and procedures created to protect Protected Client Data.

Duty Specific Training: Privacy training shall be appropriate to the tasks that each employee performs. In the case where an employee does not come into contact with Protected Client Data as a normal course of the employee's duties, the employee shall be trained on the corporate policies and procedures.

New Employees: New employees shall be trained on the corporate policies and procedures as part of their normal employment process and shall be trained on our Privacy policies and procedures, if applicable, within 30-day of being employed by SL Goodell Insurance Services Inc. The Privacy Officer shall document this training and provide the Privacy Officer with documentation of this training, within the 30-days period.

SL Goodell Insurance Services Inc. Transfers: When an employee transfers from one department to another, the employee shall be trained on our Privacy policies and procedures within 30-days of be assigned. The Privacy Officer shall document this training and provide the Privacy Office with documentation of this training, within the 30-days period.

Material Change in Policies and Procedures: when a material change in the policies and procedures occurs, each employee shall receive training on such changes within 30-days of the implementation of the change. The Privacy Officer shall document this training and provide the Privacy Office with documentation of this training, within the 30-days period.

6.0 Enforcement:

Any employee found to have violated this policy shall be subject to disciplinary action, up to and including termination of employment. In the case where inappropriate access, use or disclosure of Protected Client Data was or may have been involved, such individuals may additionally be reported to the appropriate enforcement agencies.