SECOVA™

Data Protection and Privacy Policy

Marketing Copy

1. Purpose

The purpose of this document is to

- outline the policy of Secova and each of its direct and indirect subsidiaries regarding direct communications to the public and/or specific employees to ensure compliance with California Senate Bill 168; Use of Social Security Numbers ("SB 168"), and California Civil Code section 1798.85(a) and the Department of Health and Human Services, Office of the Secretary, 45 CFR Parts 160 and 164, Standards for Privacy of Individually Identifiable Health Information
- protect important records from loss, destruction, falsification and maintain privacy in accordance with statutory, regulatory, contractual and business requirements.

2. Scope

This policy applies to all employees of Secova and any of its subsidiaries. Human Resources and the Chief Executive Officer ("CEO") are responsible for working with the Board of Directors to ensure that the Privacy Protection policy is adhered to. **Policy Enforcement:** All policy additions, modifications, and deletions are subject to review for appropriateness and approval by Secova's Privacy Officer, CTO and the Board of Directors. **Responsibility:** The Director of Human Resource, Privacy Officer, and the CEO are responsible for the interpretation, administration, and enforcement of this policy.

This Privacy Policy is effective April 1, 2003 and is the responsibility of the Privacy Officer, who may amend it, in any respect, as he or she deems necessary or appropriate from time to time with the approval of the Chief Operations Officer.

3. Principle

A number of countries have introduced legislation placing controls on the collection, processing and transmission of personal data. Depending on the respective national legislation controls may impose duties on those collecting, processing and disseminating personal information and restrict the ability to transfer that data to other countries. Data Protection and privacy is achieved by

- Implementing controls specified by the national laws on data protection and privacy.

4. Policy

It is the policy of Secova to comply with the regulations stipulated in HIPAA, SB 168 and Civil Code section 1798.85(a). Secova's Privacy Protection policy includes physical information access, posted information, print, facsimiles, electronic communications, telephone exchanges, and mail.

This policy covers all Social Security Numbers, medical records and other individually identifiable health information held or disclosed by a covered entity, in any form, whether communicated electronically, on paper, or orally.

Secova considers maintaining the security and confidentiality of Protected Health Information (PHI) and Social Security Numbers (SSN) a matter of its highest priority. Each person accessing Secova data and resources holds a position of trust relative to this information and must recognize the responsibilities entrusted in preserving the security and confidentiality of this information. The following conditions apply to all those having access to Protected Health Information and Social Security Numbers.

While Secova strives to hire employees of high integrity, Secova establishes policies, practices, and standards in order to comply with various federal and state regulations. Employees who engage in conduct that violates Company policies, practices, or standards or whose performance is unsatisfactory may be subject to corrective action (up to and including termination).

Standards

1. Physical Access Safeguards and Clean Desk Practices

a) Posted Information: Employees may not publicly post or display in any manner an individual's Social Security Number. This means that employees may not communicate or otherwise make available to the general public an individual's Social Security Number.

b) Print: A Responsible Employee must take reasonable steps to ensure that all print jobs containing PHI are retrieved and viewed only by a Responsible Employee. Employees may not print an individual's Social Security Number on any card, ID, or badge required for the individual to access products or services provided by the company.

c) Facsimiles: A Responsible Employee must take reasonable steps to ensure that all incoming faxes containing PHI are retrieved and viewed only by a Responsible Employee. In the course of performing ministerial tasks on behalf of our employer clients, Secova employees may need to send to third parties information containing Social Security Number[s] for verification, enrollment, eligibility and administrative purposes. Employees may forward this information to third parties provided the purpose for which information containing Social Security Numbers[s] is clearly stated and Secova's HIPAA and SB168compliant Facsimile cover sheet is utilized in the transmission at all times.

d) Shredding of Printed Materials and Handwritten Notes: Any Secova employee that provides services to a member must promptly shred, or store in a secure place until shredding is appropriate, any notes that contain a member's name, Social Security Number, benefits information, protected health information or any other applicable personal information.

e) Computer Protocol: All employees must lock their computer when stepping away from their desk.

f) Secured Areas: All Secova offices are considered "secured areas" and must be treated as such. Any visitor to an office must be greeted by the receptionist or employee on duty and will be issued a "Visitor" pass. All doors that open to the general public are locked at all times and opened with an employee key card. To this end, the door opening to the lobby from the Call Center is to be kept shut at all times.

2.Phone Correspondence Safeguards:

Employees may not ask for an individual's Social Security Number for identification. Instead they must ask for the individual's name, address, or any other identifier. Should there be further need for to use his/her Social Security Number, only the last four digits of the Social Security Number should be requested to complete the identification process. (See list below for other qualifying information.)

3. Non-member Authorization to Release Information:

Any release of member information must be pre-approved by the member on the "Authorization for Release of Health Information" form or by requiring the caller to provide any and/or all of the following information:

- ✓ Last 4-digits of Social Security Number
- ✓ Employee Number
- ✓ Date of Birth
- ✓ Address
- ✓ Relation to Member
- ✓ Employer Name
- ✓ Dependants' Names
- ✓ Dependants' Dates of Birth

4. Electronic Communications

a) Emails and Data Files: Employees may not transmit or require an individual to transmit his or her Social Security Number over the Internet, unless the connection is secure or the Social Security Number is encrypted. The use of password-protected documents is also acceptable, as long as the password is kept secure.

b) Internet Web Sites: Employees may not utilize or require an individual to utilize his or her Social Security Number to access an Internet Web site, unless a password or a unique personal identification number ("PIN") or other authentication device is also required to access the Web site.

5. Electronic Access to Member Information

a) Safeguards of Historic information: Access to this information is limited to select team. The information is accessible on a secured application and restricted to those with the correct user id and password.

b) CRM Usage and Safeguards: All member and/or client calls are documented on the Secova CRM system. The CRM system tracks the following information:

- ✓ Member
- ✓ Client
- ✓ Carrier
- ✓ Reason for call
- ✓ Topic of call
- ✓ Duration of call
- ✓ Status of call
- ✓ Resolution of call
- ✓ Secova employee taking call
- ✓ Any other pertinent information

c) Disclosure of Confidential Medical Information: Any electronic CRM file that contains protected health information will be indicated with a flag on the record to alert the Secova employee to request verbal confirmation of the member's identification or a written authorization to release information to a third party. When documenting such information into the CRM system an alert must be activated. Protected health information includes, but is not limited to the following:

- High Blood Pressure
- Heart, Liver and/or Kidney Disease
- Diabetes
- Mental Illness
- Prescription Medications
- HIV Testing Results
- Herpes or Hepatitis Diagnosis

Individual health information provided to an employer by or on behalf of an employee in connection with verifying an absence from employment, request for a reasonable accommodation of a disability, workers compensation claim, or other employment-related purpose, is not subject to this Privacy Policy.

6. Mail

Employees may not print an individual's Social Security Number on any materials that are mailed to the individual, unless state and federal law requires the Social Security Number to be on the document to be mailed. Notwithstanding this provision, check your department administrative and work flow procedures regarding the printing of Social Security Numbers on certain documents.

Mail addressed to a Health Plan (or known to relate to a Health Plan) and sent to Secova must be delivered to a Responsible Employee. Any other correspondence addressed to the Company that contains PHI must be forwarded to a Responsible Employee. Mail likely to contain PHI sent to a Business Associate shall be handled and processed in accordance with the guidelines established by the Business Associate to reasonably assure compliance with the Privacy Policy. Mail containing PHI should be handled and stored in accordance with the same general guidelines.

Procedures

1. Protected Health Information (PHI) and Social Security Number (SSN) Confidentiality

The following procedures must be followed to maintain client confidentiality:

a) Collect SSNs preferably only where required to do so by federal or state law.

b) When collecting PHI and/or SSNs is allowed, but not required, by law, do so only as reasonably necessary for the proper administration of lawful business activities.

c) If a unique personal identifier is needed, we will develop our own or work with the client to use their own identifiers as a substitute for the SSN.

2. Inform individuals when you request their SSNs

a) Whenever you collect PHI and/or SSNs as required or allowed by law, inform the individuals of the purpose of the collection, the intended use, and the consequences of not providing the number.

b) Any conversations with members or clients must be conducted in a tone that is professional and low to prevent them from being overheard by other Secova employees/visitors.

3. Elimination of public display of PHI and SSNs

a) Do not put PHI and/or SSNs on documents that are widely seen by others, such as identification cards, badges, time cards, employee rosters, bulletin board postings, and other materials.

b) Do not send documents containing SSNs on them through the mail, except on applications or forms or as allowed by your department's workflow procedures.

c) When sending applications, forms or other documents required by law to carry SSNs through the mail, place the SSN where it will not be revealed by an envelope window. Where possible, leave the SSN field on forms and applications blank and ask the individual to fill it in before returning the form or application.

d) Do not send PHI and/or SSNs by email unless the connection is secure or the PHI and/or SSN are encrypted.

e) Do not require an individual to send his or her PHI and/or SSN over the Internet or by email, unless the connection is secure or the PHI and/or SSN are encrypted.

f) Do not require individuals to use SSNs as passwords or codes for access to Internet web sites or other services.

4. Control access to PHI and/or SSNs

Secova limits access to records containing PHI and/or SSNs only to those who need to see the information and numbers for the performance of their duties. Protect records containing PHI and/or SSNs, including back-ups, during storage by encrypting the numbers in electronic records or storing records in locked cabinets. Do not store records containing PHI and/or SSNs on computers or other electronic devices that are not secured against unauthorized access. Avoid sharing PHI and/or SSNs with other companies or organizations except where required by law, or authorized by the individual. If you do share PHI and/or SSNs with other companies or organizations, including contractors, use written agreements to protect their confidentiality.

Prohibit such third parties from re-disclosing SSNs, except as required by law.

Require such third parties to use effective security controls on record systems containing SSNs.

Hold such third parties accountable for compliance with the restrictions you impose, including monitoring or auditing their practices.

NOTE: If PHI and/or SSNs are disclosed inappropriately and the individuals whose PHI and/or SSNs were disclosed are put at risk of identity theft or other harm, promptly notify your manager or Compliance Officer immediately.

5. Employee Commitment

When handling confidential information, each employee is held responsible to:

a) Respect the privacy and rules governing the use of any information accessible through the computer system or network and only utilize information necessary for performance of employee's job.

b) Respect the ownership of proprietary software. For example, do not make unauthorized copies of such software for your own use, even when the software is not physically protected against copying.

c) Respect the finite capability of the systems, and limit use so as not to interfere unreasonably with the activity of other users. d) Respect the procedures established to manage the use of the system. e) Prevent unauthorized use of any information in files maintained, stored, or processed by Secova f) Do not seek personal benefit or permit others to benefit personally by any confidential information or use of equipment available through employee's work assignment. g) Adhere to all stated policies; including but not limited to the Privacy Protection Policy and any specific departmental guidelines. h) Do not operate any non-licensed software on any computer provided by Secova i) Do not exhibit or divulge the contents of any record or report except to fulfill a work assignment and in accordance with Secova policy. j) Do not knowingly include or cause to be included in any record or report, a false, inaccurate, or misleading entry. k) Do not remove PHI and/or SSNs from the office where it is kept except in the performance of employee's duties.

l) Understand that the information accessed through all Secova information systems contains sensitive and confidential patient/member care, business, financial and hospital employee information, which should only be disclosed to those, authorized to receive it.

m) Do not release any authentication code or device to anyone else, or allow anyone else to access or alter information under employee's identity. n) Do not utilize other employee's authentication code or device in order to access any Secova system. o) Do not write user id and passwords on paper and leave unsecured. p) Respect the confidentiality of any reports printed from any information system containing patient/member information and handle, store and dispose of these reports appropriately. q) Do not divulge any information that identifies PHI and/or SSNs. r) Understand that all access to the system will be monitored. s) Sign the Privacy Protection Policy Acknowledgement. t) Terms of policy extend two-year post termination.

Definitions

Business Associate: "Business Associate" shall mean, Secova and its subsidiaries, a person or entity, which performs or assists in the performance of a function or activity involving the use or disclosure of PHI from or on behalf of a Health Plan. Such functions or activities include claims processing or administration, data analysis, utilization review, quality assurance, billing, benefit management, re-pricing, and other professional services. "Business Associate" will include all employees of the Business Associate who perform or assist in the performance of functions on behalf of a Customer

Covered Entity: "Covered Entity" shall mean a health plan, a health care clearinghouse, or a Health Care Provider who transmits any health information in electronic form in connection with a transaction covered by HIPAA.

Proprietary Information: shall mean information relating to Secova and its Clients that is not generally known to the public, including be not limited to information that relates to past, present, or future research and development, trade secrets, products and services, pricing, marketing,

financial matters, or business affairs (including policies, procedures, plans, and methods or operation).

Protected Health Information (PHI): means individually identifiable health information that (a) relates to the past, present, or future physical or mental condition of an Individual, provision of health care to an Individual, or payment for such health care; (b) can either identify the Individual or there is a reasonable basis to believe the information can be used to identify the Individual; and (c) is received or created by or on behalf of a Customer.

Electronic Transmissions includes transactions using all forms of electronic media. Such transactions include the transfer of information over the Internet (wide-open), Extranet (using Internet technology to link a business with information only accessible to collaborating parties), leased lines, dial-up lines, and private networks. Electronic media includes magnetic tape, disk or compact disc media. Telephone voice response and "fax back" (a request for information made via voice using a fax machine and requested information returned via that same machine as a fax) systems and facsimile transmissions are not included.

Privacy Officer. The person designated by Secova as responsible for implementing and updating the Privacy Policy and for carrying out the duties assigned to him or her under the Privacy Policy. Reference to the Privacy Officer includes any person(s) to whom the Privacy Officer has made an applicable delegation under this policy.

Responsible Employee: An employee of Secova whose duties (a) require that the employee have access to PHI for purposes of Secova Operations, or (b) make it likely that he or she will receive or have access to PHI. Any employee who receives PHI from, or on behalf of Secova, even though his or her duties do not (or are not expected to) include receiving PHI; will be treated as a Responsible Employee under the Privacy Policy.