

CENTRAL STATE COMMUNITY SERVICES OKLAHOMA

**POLICIES FOR PROTECTION OF THE PRIVACY
OF
PROTECTED HEALTH INFORMATION**

Effective: April 14, 2003

CENTRAL STATE COMMUNITY SERVICES OKLAHOMA

**POLICIES FOR PROTECTION OF THE PRIVACY
OF
PROTECTED HEALTH INFORMATION**

TABLE OF CONTENTS

I.	INTRODUCTION	1
A.	Purpose of These Privacy Policies.....	1
B.	Disclaimer	1
II.	PROTECTED HEALTH INFORMATION	1
A.	What is	1
B.	De-Identification of Health Information	2
1.	De-Identification	2
2.	Requirements for De-Identification	2
3.	Requirements for Re-Identification	4
III.	ADMINISTRATIVE POLICIES.....	5
A.	Designation of Privacy Official	5
1.	Designation	5
2.	Documentation.....	5
B.	Designation of Other Persons	5
1.	Person/Office to Receive Complaints.....	5
2.	Person/Office to Receive and Process Requests for Access.....	5
3.	Person/Office to Receive and Process Requests for Amendment	6
4.	Documentation.....	6
C.	Identification of Workforce Members’ Access To Protected Health Information	6
D.	Training of Workforce	6
E.	Safeguards to Protect the Privacy of Protected Health Information	7
F.	Receipt of Notice of Amended Protected Health Information.....	7
G.	Process for Individuals to Make Complaints	7
H.	Sanctions	7
I.	Mitigation of Harmful Effect.....	8
J.	Prohibition on Intimidating or Retaliatory Acts	8
1.	Individuals.....	8
2.	Individuals and Others	8
K.	Prohibition on Waiver of Rights	8
L.	Changes to Policies and Procedures	9

1.	Changes in Law.....	9
2.	Changes to Privacy Practices Stated In Notice of Privacy Practices	9
3.	Changes to Privacy Practices Not Stated In Notice of Privacy Practices .	10
M.	Documentation.....	10
N.	Period of Retention	10
O.	Business Associates	10
P.	Reporting Violations.....	11
Q.	Questions Concerning HIPAA Compliance	11
R.	Action by Designee.....	11
IV.	CSCSO REQUESTS FOR PROTECTED HEALTH INFORMATION.....	11
A.	Generally.....	11
B.	Routine and Recurring Requests.....	12
C.	Other Requests.....	12
V.	NOTICE OF PRIVACY PRACTICES.....	12
A.	Form of Notice of Privacy Practices.....	12
B.	Provision of Notice of Privacy Practices	13
1.	To Each Individual.....	13
2.	Posting	13
3.	Web Site.....	13
C.	Obtaining Acknowledgment of Receipt of Notice of Privacy Practices.....	13
D.	Revision of Notice of Privacy Practices	14
E.	Documentation.....	14
VI.	USES AND DISCLOSURE OF PROTECTED HEALTH INFORMATION	14
A.	General Rule	14
B.	Incidental Uses and Disclosures.	14
C.	Use and Disclosure of Only the Minimum Necessary Information.....	15
1.	General Rule	15
2.	Exceptions to Minimum Necessary Requirement.....	15
3.	Routine and Recurring Disclosures	15
4.	Other Disclosures.....	15
5.	Permitted Reliance	16
D.	Uses and Disclosures to Carry Out Treatment, Payment and Health Care Operations.....	16
E.	Uses and Disclosures for Which an Authorization is Required.....	17
1.	General Rule	17
2.	What is a Valid Authorization?.....	18
3.	Maintaining an Authorization.....	18
4.	Conditioning of Authorizations	19
5.	Form of Authorization	19
6.	Compound Authorizations.....	21
7.	Revocation of an Authorization	22
8.	Documentation.....	22

F.	Uses and Disclosures Requiring an Opportunity for the Individual to Agree or to Object.....	22
1.	General Rule	22
2.	Persons Involved in the Individual's Care	22
3.	Disaster Relief.....	24
G.	Uses and Disclosures for which an Authorization or an Opportunity to Agree or Object is Not Required.....	24
1.	General Rule	24
2.	Uses and Disclosures Required by Law.....	25
3.	Uses and Disclosures for Public Health Activities	25
4.	Uses and Disclosures About Victims of Abuse, Neglect or Domestic Violence	28
5.	Uses and Disclosures for Health Oversight Activities.....	29
6.	Disclosures for Judicial and Administrative Proceedings	31
7.	Disclosures for Law Enforcement Purposes	34
8.	Uses and Disclosures About Decedents.....	37
9.	Uses and Disclosures for Cadaveric Organ, Eye or Tissue Donation.....	38
10.	Uses and Disclosures to Avert a Serious Threat to Health or Safety.....	38
11.	Uses and Disclosures for Specialized Government Functions	40
12.	Disclosures for Workers' Compensation	42
13.	Disclosure to the Secretary of Health and Human Services	42
14.	Disclosures by Whistleblowers.....	43
15.	Disclosures by Workforce Members Who are Victims of a Crime	44
16.	Disclosures to Business Associates	44
H.	Uses and Disclosures for Marketing.....	45
1.	General Rule	45
2.	Exceptions.....	45
3.	"Marketing" Defined	45
I.	Uses and Disclosures for Fundraising.....	46
1.	General Rule	46
2.	Opting Out	46
J.	Limited Data Set	47
1.	General Rule	47
2.	Permitted Uses	47
3.	Data Use Agreement	48
4.	"Limited Data Set" Define	47
K.	Verification of Identity and Authority.....	48
1.	General Rule	48
2.	Personal Representatives	49
3.	Conditions on Disclosures	49
4.	Identity of Public Officials.....	50
5.	Authority of Public Officials	50
6.	Exercise of Professional Judgment.....	50
L.	Prior Authorizations.....	51
1.	General Rule	51

2.	Effect of Prior Authorization for Purposes Other Than Research	51
VII.	RIGHTS OF INDIVIDUALS	51
A.	Right to Request Privacy Protection	51
1.	Restriction of Uses and Disclosures	51
2.	Restriction on Means and Location of Communications.....	53
B.	Right of Access	53
1.	Generally.....	53
2.	Request for Access.....	53
3.	Action on Request for Access.....	54
4.	Providing Access	54
5.	Denial of Access	56
6.	Actions if Access is Denied	57
7.	Documentation.....	58
C.	Right to Request Amendment.....	59
1.	Generally.....	59
2.	Request for Amendment.....	59
3.	Action on Request for Amendment	59
4.	Accepting the Amendment	60
5.	Grounds for Denying the Amendment.....	61
6.	Actions if Amendment is Denied.....	61
7.	Documentation.....	63
D.	Right to an Accounting of Disclosures	63
1.	Right to Accounting.....	63
2.	Content of the Accounting.....	65
3.	Provision of the Accounting	67
VIII.	PERSONAL REPRESENTATIVES	68
A.	General Rule	68
B.	Adults and Emancipated Minors.....	68
C.	Unemancipated Minors.....	68
1.	General Rule	68
2.	Exception.	69
D.	Deceased Individuals	70
E.	Abuse, Neglect, Endangerment Situations.....	70
IX.	DEFINITIONS.....	70
A.	Authorized Member of CSCSO’s Workforce.....	70
B.	Business Associate.....	71
C.	Covered Entity	71
D.	Designated Record Set.....	71
E.	Disclosure	72
F.	Health Care Operations.....	72
G.	Health Care	73
H.	Health Oversight Agency.....	73

I.	HIPAA Privacy Rule.....	73
J.	Inmate	74
K.	Law Enforcement Official	74
L.	Payment.....	74
M.	Personal Representative	75
N.	Secretary of Health and Human Services	75
O.	These Privacy Policies	75
P.	Treatment	75
Q.	Use	75
R.	Workforce	75

CENTRAL STATE COMMUNITY SERVICES OKLAHOMA

POLICIES FOR PROTECTION OF THE PRIVACY OF PROTECTED HEALTH INFORMATION

I. INTRODUCTION

A. Purpose of These Privacy Policies.

These privacy policies for the protection of the privacy of protected health information are intended to comply with the requirements of the federal Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), regulations under HIPAA, and any applicable state law that is more stringent than the HIPAA requirements. They are designed to comply with the standards, implementation specifications, and other requirements of the HIPAA security and privacy regulations at 45 CFR Part 160 and Part 164.

In all instances, these privacy policies shall be interpreted and construed consistent with the requirements of HIPAA, its regulations, and any more stringent state law.

In the event of any conflict between a provision of these privacy policies and a requirement of HIPAA, a regulation under HIPAA, or a more stringent state law, that HIPAA, HIPAA regulation, or state law requirement shall control.

B. Disclaimer.

All of the policies contained or referred to in these privacy policies, or that may be added or otherwise established by CSCSO in the future, represent the policies established by CSCSO for the members of its workforce in relation to the particular subject addressed by the policy. It is the intention of CSCSO that these privacy policies be used by its employees, and other members of its workforce, in meeting their responsibilities to CSCSO. Violation of a policy can be the basis for discipline or termination of employment; however, because these privacy policies relate to the establishment and maintenance of high standards of performance, under no circumstances shall any policy be interpreted or construed as establishing a minimum standard, or any evidence of a minimum standard, of the safety, due care, or any other obligation which may be owed by CSCSO, its employees, or its agents to another person.

II. PROTECTED HEALTH INFORMATION.

A. What is “Protected Health Information”?

“Protected health information” is any health information maintained by CSCSO that is individually identifiable except employment records held by CSCSO in its role as an employer.

“Individually identifiable health information” means any health information, including demographic information, whether oral or recorded in any form or medium, including demographic information collected from an individual, that:

1. Is created or received by health care provider, a health plan, employer, or health care clearinghouse;
2. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and,
3. That identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

All health information maintained by CSCSO is individually identifiable unless and until it is de-identified as stated in Section II.B, below.

B. De-Identification of Health Information.

1. De-Identification.

Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information.

2. Requirements for De-Identification.

Before any member of CSCSO’s workforce treats any information as being de-identified, it must be submitted to the Privacy Officer. Whether or not health information has been de-identified will be determined by the Privacy Officer.

The Privacy Officer may find that health information has been de-identified only if one of the following two conditions is met:

a. Condition 1: Statistical and Scientific Principles.

A person with appropriate knowledge and experience with

generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:

- (1) Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is subject to the information; and,
- (2) Documents the methods and results of the analysis that justify such determination. Such documentation shall be in accordance with the requirements stated in Section III.M (see, Page 10) and Section III.N (see, Page 10) of these privacy policies.

b. Condition 2: Removal of Identifiers.

The following identifiers of the individual or of relatives, employers, or household members of the individual are removed and CSCSO does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information:

- (1) Names;
- (2) All geographic subdivisions smaller than a State, including street addresses, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicity available data from the Bureau of the Census:
 - (a) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
 - (b) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people are changed to 000.
- (3) 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;

- (4) Telephone numbers;
- (5) Fax numbers;
- (6) Electronic mail addresses;
- (7) Social security numbers;
- (8) Medical record numbers;
- (9) Health plan beneficiary numbers;
- (10) Account numbers;
- (11) Certificate/license numbers;
- (12) Vehicle identifiers and serial numbers, including license plate numbers;
- (13) Device identifiers and serial numbers;
- (14) Web Universal Resource Locators (URLs);
- (15) Internet Protocol (IP) address numbers;
- (16) Biometric identifiers, including finger and voice prints;
- (17) Full face photographic images and any comparable images; and,
- (18) Any other unique identifying number, characteristic, or code, except as permitted by Section II.B.3 (see, Page 4) of these privacy policies.

3. Requirements for Re-Identification.

A code or other means of record identification may be assigned to allow information de-identified to be re-identified by CSCSO provided:

- a. The code or other means of record identification shall not be derived from or related to information about the individual and shall not otherwise be capable of being translated so as to identify the individual; and,
- b. The code or other means of record identification shall not be used

or disclosed for any other purpose and the mechanism for re-identification shall not be disclosed.

Whether or not information shall be coded for re-identification and be re-identified shall be determined by the Privacy Officer. If information is re-identified, the Privacy Officer shall oversee the process of doing so.

III. ADMINISTRATIVE POLICIES

A. Designation of Privacy Official.

1. Designation.

CSCSO's Executive Program Director shall designate a privacy official who shall be responsible for the development, updating and implementation of CSCSO's privacy policies. That privacy official shall be called the "Privacy Officer" of CSCSO.

2. Documentation.

CSCSO's Executive Program Director shall maintain, or cause to be maintained, a written or electronic record of the designation of the Privacy Officer. Such record shall be maintained for six (6) years from the date of its creation or the date it is last in effect, whichever is later.

B. Designation of Other Persons.

1. Person/Office to Receive Complaints.

CSCSO's Chief Executive Officer shall designate a contact person or office who shall:

- a. Be responsible for receiving complaints concerning CSCSO's privacy policies and procedures, CSCSO's compliance with those policies and procedures, or CSCSO's compliance with the HIPAA privacy rule pursuant to Section III.G (see, Page 7) of these privacy policies; and,
- b. Provide further information about matters covered by CSCSO's Notice of Privacy Practices.

2. Person/Office to Receive and Process Requests for Access.

CSCSO's Executive Program Director shall designate a contact person or office who shall be responsible for receiving and processing individuals'

requests for access to protected health information pursuant to Section VII.B “Right of Access” (see, Page 53) of these privacy policies.

3. Person/Office to Receive and Process Requests for Amendment.

CSCSO’s Executive Program Director shall designate a contact person or office who shall be responsible for receiving and processing individuals’ requests for amendment of protected health information pursuant to Section VII.C “Right to Request Amendment” (see, Page 58) of these privacy policies.

4. Documentation.

CSCSO’s Executive Program Director shall maintain, or cause to be maintained, a written or electronic record of the title of the person or office for each person or office designed under this Section III.C. Such record shall be maintained for six (6) years from the date of its creation or the date it was last in effect, whichever is later.

C. Identification of Workforce Members’ Access to Protected Health Information.

Attached to these privacy policies as Appendix A is an identification of those classes of CSCSO’s workforce who need access to protected health information to carry out their duties and, for each of those classes, the category or categories of protected health information to which access is needed and any conditions appropriate to that access. Failure of a member of the workforce to comply with that access or those conditions will result in disciplinary action up to and including termination of employment.

D. Training of Workforce.

All members of CSCSO’s workforce shall be trained on CSCSO’s policies and procedures with respect to protected health information as necessary and appropriate for the members of the workforce to carry out their functions within CSCSO.

Each member of the workforce on April 14, 2003, shall be trained by no later than Nov. 1, 2003. Thereafter, each new member of the workforce shall be trained during new employee orientation within ninety (90) calendar days after the person joins the workforce. Each member of the workforce whose functions are affected by a material change in these privacy policies or procedures shall be trained within ninety (90) calendar days after the material change becomes effective.

Documentation of the training for each member of the workforce shall be kept in

written or electronic form for six (6) years after the date of its creation or the date that person ceases to be a member of CSCSO's workforce, whichever is later.

E. Safeguards to Protect the Privacy of Protected Health Information.

The Privacy Officer shall implement appropriate administrative, technical and physical safeguards to protect the privacy of protected health information and to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.

F. Receipt of Notice of Amended Protected Health Information.

Any member of CSCSO's workforce who is informed by another health care provider, health plan or a healthcare clearinghouse of an amendment to an individual's protected health information shall promptly inform the Privacy Officer of the amendment. The Privacy Officer shall cause the protected health information concerning that individual that is maintained by CSCSO to be amended as stated in Section VII.C.4.a "Making the Amendment" (see, Page 60) of these privacy policies.

G. Process for Individuals to Make Complaints.

Individuals who desire to make a complaint against CSCSO concerning CSCSO's privacy policies and procedures, its compliance with those policies and procedures, or the requirements of the HIPAA privacy rule shall submit the complaint in writing to the Privacy Officer at the CSCSO main office.

The Privacy Officer shall investigate the complaint and respond to the individual in writing concerning his or her findings and what action, if any, CSCSO will take in response to the complaint.

The Privacy Officer shall cause written documentation of each complaint and its disposition to be kept in written or electronic form for six (6) years after the date of its creation or the date when it was last in effect, whichever is later.

H. Sanctions.

Except for actions that are covered by and meet the conditions of Section VI.G.14 "Disclosures by Whistleblowers" (see, Page 43), Section VI.G.15 "Disclosures by Workforce Members Who are Victims of a Crime" (see, Page 44), or Section III.J "Prohibition on Intimidating or Retaliatory Acts" (see, Page 8) of these privacy policies, any member of CSCSO's workforce who fails to comply with CSCSO's privacy policies and procedures or the requirements of the HIPAA privacy rule shall be subject to sanctions imposed through CSCSO's discipline and discharge policies.

The Privacy Officer shall cause written documentation of the sanctions that are applied, if any, to be kept in written or electronic form for six (6) years after the date of its creation or the date when it is last in effect, whichever is later.

I. Mitigation of Harmful Effect.

If there is a use or disclosure of protected health information by a member of CSCSO's workforce or a CSCSO business associate in violation of CSCSO's privacy policies or the requirements of the HIPAA privacy rule, the Privacy Officer shall mitigate, or cause to be mitigated, to the extent practicable, any harmful effect that is known to CSCSO.

J. Prohibition on Intimidating or Retaliatory Acts.

Neither CSCSO nor any member of CSCSO's workforce may intimidate, threaten, coerce, discriminate against, or take other retaliatory action against:

1. Individuals.

Any individual for the exercise by the individual of any right under, or for participation by the individual in any process established by, these privacy policies or the HIPAA privacy rule, including filing a complaint under the HIPAA privacy rule or under these privacy policies.

2. Individuals and Others.

Any individual or other person for:

- a. Filing of a complaint with the Secretary of Health and Human Services under the HIPAA privacy rule;
- b. Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing under the Administrative Simplification provisions of HIPAA; or
- c. Opposing any act or practice made unlawful by the HIPAA privacy rule, provided the individual or person has a good faith belief that the practice opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of protected health information in violation of the HIPAA privacy rule.

K. Prohibition on Waiver of Rights.

No member of CSCSO's workforce may require an individual to waive the individual's rights under these privacy policies or the HIPAA privacy rule as a

condition for the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

L. Changes to Policies and Procedures.

1. Changes in Law.

The Privacy Officer shall promptly change these privacy policies as necessary and appropriate to comply with changes in the law, including changes in the HIPAA privacy rule. The changed policy or procedure shall be promptly documented and implemented. If the change materially affects the content of CSCSO's Notice of Privacy Practices, the Privacy Officer shall promptly make the appropriate revisions to the notice in accordance with Section V.D "Revision of Notice of Privacy Practices" (see, Page 14) of these privacy policies.

2. Changes to Privacy Practices Stated In Notice of Privacy Practices.

When CSCSO changes a privacy practice that is stated in its Notice of Privacy Practices and makes corresponding changes to CSCSO's policies, the change shall be effective for protected health information CSCSO created or received prior to the effective date of the notice revision provided:

- a. The Privacy Officer ensures that the policy or procedure, as revised to reflect the change, complies with the HIPAA privacy rule;
- b. The Privacy Officer documents the policy or procedure, as revised, as stated in Section III.M "Documentation" (see, Page 10) and Section III. N "Period of Retention" (see, Page 10) of these privacy policies; and,
- c. The Privacy Officer revises the Notice of Privacy Practices to state the changed practice and makes the revised notice available as stated in Section V.B "Provision of Notice of Privacy Practices" (see, Page 13) of these privacy policies. The changed practice may not be implemented prior to the effective date of the revised Notice of Privacy Practices.

If these conditions are not met, then the change is effective only with respect to protected health information created or received after the effective date of the revised Notice of Privacy Practices.

3. Changes to Privacy Practices Not Stated In Notice of Privacy

Practices.

CSCSO may change, at any time, a privacy practice that does not materially affect the content of the Notice of Privacy Practices, provided:

- a. The policy or procedure involved, as revised, complies with the HIPAA privacy rule; and,
- b. Prior to the effective date of the change, the policy or practice, as revised, is documented by the Privacy Officer by causing it to be kept in written or electronic form.

M. Documentation.

The Privacy Officer shall take, or cause to be taken, each of the following actions:

- a. Maintain these privacy policies and procedures in written or electronic form;
- b. If a communication is required by these privacy policies and procedures, or by the privacy rule, to be in writing, maintain that writing, or an electronic copy, as documentation;
- c. If an action, activity, or designation is required by these privacy policies and procedures, or by the privacy rule, to be documented, maintain a written or electronic record of that action, activity or designation.

N. Period of Retention.

Documentation required by Section III.M “Documentation”, above, shall be retained for six (6) years from the date of its creation or the date when it last was in effect, whichever is later.

O. Business Associates.

Prior to CSCSO disclosing any protected health information to a business associate or allowing a business associate to create or receive protected health information on its behalf, the Privacy Officer shall obtain satisfactory assurance from the business associate that the business associate will appropriately safeguard the protected health information disclosed to it or that it creates or receives on CSCSO’s behalf. The satisfactory assurance shall be through a written contract with the business associate that contains at least all the provisions required by the privacy rule.

However, if the business associate is required by law to perform a function or activity on behalf of CSCSO or to provide a service described in the HIPAA privacy rule's definition of a business associate (see, Section IX.B, "Business Associate" on Page 71 of these privacy policies) to CSCSO, CSCSO may disclose protected health information to the business associate to the extent necessary to comply with the legal mandate without meeting the requirements for business associates, provided:

1. CSCSO attempts in good faith to obtain satisfactory assurances, as stated above; and,
2. If that attempt fails, the Privacy Officer documents the attempt and the reasons that the assurances cannot be obtained.

Any contract of CSCSO where the other party, or one of the other parties, may be a business associate shall be submitted to the Privacy Officer for review for compliance with these privacy policies and the HIPAA privacy rule prior to being signed on behalf of CSCSO.

P. Reporting Violations.

Each member of CSCSO's workforce must report any actual or possible violation of CSCSO's privacy policies or the HIPAA privacy rule to the Privacy Officer as soon as he or she becomes aware of the actual or possible violation.

Q. Questions Concerning HIPAA Compliance.

If any member of CSCSO's workforce has a question concerning CSCSO's privacy policies, the HIPAA privacy rule, or their application to any situation, he or she should contact the Privacy Officer for guidance. The Privacy Officer may contact legal counsel for legal advice as he or she believes is necessary or desirable.

R. Action by Designee.

Whenever an action may be or is required to be taken under these privacy policies by the Privacy Officer or any other member of CSCSO's workforce, the action may be taken by that person's designee.

IV. CSCSO REQUESTS FOR PROTECTED HEALTH INFORMATION.

A. Generally.

When requesting protected health information from another health care provider, a health plan or a health care clearinghouse, a member of CSCSO's workforce

must limit the request to that which is reasonably necessary to accomplish the purpose for which the request is made.

Except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the request, members of CSCSO's workforce may not request an entire medical record.

B. Routine and Recurring Requests.

For a request that is made on a routine and recurring basis, the Privacy Officer shall from time to time develop and implement standard protocols that limit the protected health information requested to the amount that is reasonably necessary to accomplish the purpose for which the request is made.

C. Other Requests.

Whenever any member of CSCSO's workforce desires to request protected health information from another provider, a health plan or a health care clearinghouse and the request is not one made pursuant to a protocol for routine and recurring requests, he or she shall first submit the request to the Program Coordinator, Home Supervisor or Health Care Coordinator for review and approval prior to the request being made. The PC, HC or HCC shall review the request on an individual basis using the following criteria to limit the request to the information reasonably necessary to accomplish the purpose for which the request is made:

The criteria to be applied are:

- a. Whether or not the information requested is related to the purpose of the request.
- b. Whether or not the information requested will assist in the accomplishment of the purpose of the request.
- c. Whether or not the purpose of the request can be accomplished without the information requested.
- d. Whether or not the purpose of the request can be met with information that is not protected health information.

V. NOTICE OF PRIVACY PRACTICES.

A. Form of Notice of Privacy Practices.

The Notice of Privacy Practices used by CSCSO shall be established from time to time by the Privacy Officer and shall meet the requirements of the HIPAA

privacy regulations.

B. Provision of Notice of Privacy Practices.

1. To Each Individual.

a. Generally.

Except in an emergency treatment situation, CSCSO's Notice of Privacy Practices shall be provided to any individual who receives services or supports from CSCSO (except to an inmate of a correctional institution) no later than the date of the first service delivery by CSCSO and to other persons upon request. In an emergency treatment situation, CSCSO's Notice of Privacy Practices shall be provided as soon as reasonably practicable after the emergency treatment situation.

The Notice of Privacy Practices also shall be made available at CSCSO's office(s) for individuals to request to take with them.

b. Via E-Mail.

If the individual agrees and that agreement has not been withdrawn, the Notice of Privacy Practices will be provided to that individual by e-mail in lieu of physical delivery. If the e-mail transmission fails, a paper copy of the Notice of Privacy Practices will be provided to the individual. An individual who receives electronic notice may still obtain a paper copy of the notice upon request.

2. Posting.

CSCSO's Notice of Privacy Practices shall be prominently posted in the reception areas of the CSCSO's offices.

3. Web Site.

CSCSO's Notice of Privacy Practices shall be prominently posted on CSCSO's web site and made available electronically through the web site.

C. Obtaining Acknowledgment of Receipt of Notice of Privacy Practices.

Except in an emergency treatment situation, the CSCSO staff member who provides CSCSO's Notice of Privacy Practices to an individual in conjunction with the date of first service delivery as stated shall obtain a written

acknowledgment of the individual's receipt of the Notice of Privacy Practices. The written acknowledgment shall be filed in the individual's record.

If the individual's written acknowledgment cannot be obtained, the staff member(s) who attempted to obtain it shall document their good faith efforts to obtain the acknowledgment and the reason why it was not obtained. That documentation shall be filed in the individual's record.

D. Revision of Notice of Privacy Practices.

Whenever there is a material change to the uses or disclosures, the individual's rights, CSCSO's legal duties, or other privacy practices stated in the notice, the Privacy Officer shall cause the Notice of Privacy Practices to be promptly revised, made available on request and distributed.

Except when the material change is required by law, a material change to any term of the Notice of Privacy Practices shall not be implemented prior to the effective date of the Notice of Privacy Practices in which the material change is reflected.

E. Documentation.

A copy of each Notice of Privacy Practices used by CSCSO and of each written acknowledgment of receipt of the notice or documentation of good faith efforts to obtain such acknowledgment shall be maintained by CSCSO in written or electronic form for six (6) years after the date the notice was last in effect.

VI. USES AND DISCLOSURE OF PROTECTED HEALTH INFORMATION.

A. General Rule.

Except as otherwise stated in this Section VI, CSCSO shall obtain the individual's written authorization in accordance with these privacy policies, prior to using or disclosing protected health information concerning the individual.

B. Incidental Uses and Disclosures.

A use or disclosure that is incidental to a use or disclosure that is otherwise permitted or required by these privacy policies or the HIPAA privacy rule is permissible provided: (1) the applicable requirements of Section VI.C "Use and Disclosure of Only the Minimum Necessary Information", below; and, (2) reasonable safeguards have been applied to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure (see, Section III.E, "Safeguards to Protect the Privacy of Protected Health Information" on Page 7).

C. Use and Disclosure of Only the Minimum Necessary Information.

1. General Rule.

Except as stated in Section VI.C.2, below, when using or disclosing protected health information, members of CSCSO's workforce shall make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use or disclosure.

2. Exceptions to Minimum Necessary Requirement.

The preceding general rule concerning limiting use and disclosure of protected health information to the minimum necessary does not apply to:

- a. Disclosures to a health care provider for treatment.
- b. Uses or disclosures made to the individual.
- c. Uses or disclosures made pursuant to a written authorization in accordance with these privacy policies.
- d. Disclosures made to the Secretary of Health and Human Services in accordance with the HIPAA privacy rule.
- e. Uses or disclosures that are required by law.
- f. Uses or disclosures that are required for CSCSO's compliance with the HIPAA privacy rule.

3. Routine and Recurring Disclosures.

For any type of disclosure that is made on a routine and recurring basis, the protected health information requested is limited to the amount that is reasonably necessary to accomplish the purpose for which the disclosure is made.

4. Other Disclosures.

Any disclosures that are not covered by an established protocol shall be reviewed by the Home Supervisor, Program Coordinator, Sr. Program Coordinator, or Health Care Coordinator on an individual basis using the following criteria to limit the protected health information disclosed to the information reasonably necessary to accomplish the purpose for which disclosure is sought.

The criteria to be applied are:

- a. Whether or not the information requested is reasonably related to the purpose of the request.
- b. Whether or not the information requested will assist in the accomplishment of the purpose of the request.
- c. Whether or not the purpose of the request can be accomplished without the information requested.
- d. Whether or not the purpose of the request can be met with information that is not protected health information.

5. Permitted Reliance.

If the reliance is reasonable under the circumstances, members of CSCSO's workforce may rely on a requested disclosure as the minimum necessary for the stated purpose when:

- a. Making disclosures to public officials that are permitted under Section VI.G "Uses and Disclosures for which an Authorization or an Opportunity to Agree or Object is Not Required" (see, Page 24) of these privacy policies, if the public official represents that the information is the minimum necessary for the stated purpose(s);
- b. The information is requested by another covered entity;
- c. The information is requested by a professional who is a member of CSCSO's workforce or a business associate of CSCSO for the purpose of providing professional services to CSCSO, if the professional represents that the information requested is the minimum necessary for the stated purpose(s); or,

D. Uses and Disclosures to Carry Out Treatment, Payment and Health Care Operations.

CSCSO may use or disclose protected health information, as follows:

1. To the individual.
2. For its own treatment, payment, or health care operations.
3. For treatment activities of a health care provider.
4. To another entity covered by the privacy rule or a health care provider for the payment activities of the entity that receives the information.
5. To another entity covered by the privacy rule for health care operations of the entity that receives the information, if CSCSO and that other entity has or have had a relationship with the individual who is the subject of the protected health information being requested, the protected health information pertains to that relationship, and the disclosure is:
 - a. For conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such 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 individuals with information about treatment alternatives; and related functions that do not include treatment.
 - b. Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities
 - c. For the purpose of health care fraud and abuse detection or compliance.

E. Uses and Disclosures for Which an Authorization is Required.

1. General Rule.

Except as otherwise permitted or required by these privacy policies, CSCSO will not use or disclose protected health information without an

authorization that is valid under this Section VI.E. When CSCSO obtains or receives a valid authorization for its use or disclosure of protected health information, CSCSO's use or disclosure must be consistent with that authorization.

2. What is a Valid Authorization?

An authorization is valid if it contains all the elements required by Section VI.E.5 "Form of Authorization" (see, Page 19) of these privacy policies and it is not defective.

An authorization is defective if the document has any of the following defects:

- a. The expiration date has passed or the expiration event is known by CSCSO to have occurred.
- b. The authorization has not been filled out completely with respect to an element required to be included in the authorization;
- c. The authorization is known by CSCSO to have been revoked;
- d. The authorization lacks a required element (see, Section VI.E.5, "Form of Authorization" on Page 19) of these privacy policies);
- e. The authorization violates the requirements concerning compound authorizations (see, Section VI.E.6, "Compound Authorizations" on Page 21 of these privacy policies);
- f. The authorization violates the requirements concerning conditioning of authorizations (see, Section VI.E.4, "Prohibition on Conditioning of Authorizations" on Page 19 of these privacy policies); or,
- g. If any material information in the authorization is known by CSCSO to be false.

If any member of CSCSO's workforce believes an authorization is defective for any reason, he or she should promptly report that fact and the basis for his or her belief to the Privacy Officer.

3. Maintaining an Authorization.

All authorizations shall be filed in the individual's record.

4. Conditioning of Authorizations.

a. General Rule.

Except as stated in Section VI.E.4.b “Exceptions”, below, CSCSO will not condition treatment or payment to an individual on the receipt of an authorization from that individual.

b. Exceptions.

CSCSO may condition treatment or payment to an individual on the receipt of an authorization from that individual in the following situations:

- (1) **Research.** CSCSO may condition the provision of research-related treatment on provision of an authorization for the use or disclosure of protected health information for such research .
- (2) **Disclosure Is Sole Purpose.** CSCSO may condition the provision of health care that is solely for the purpose of creating protected health information for disclosure to a third party on provision of an authorization for the disclosure of the protected health information to that third party.

5. Form of Authorization.

a. Required Elements.

An authorization must contain at least the following elements:

- (1) A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion.
- (2) The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure.
- (3) The name or other specific identification of the person (s), or class of persons, to whom CSCSO may make the requested use or disclosure.

- (4) A description of each purpose of the requested use or disclosure. The statement “at the request of the individual” is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose.
- (5) An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. The statement “end of the research study,” “none,” or similar language is sufficient if the authorization is for a use or disclosure of protected health information for research, including for the creation and maintenance of a research database or research repository.
- (6) A statement of the individual’s right to revoke the authorization in writing and either:
 - (a) The exceptions to the right to revoke, together with a description of how the individual may revoke the authorization; or,
 - (b) To the extent that the information is stated in the Notice of Privacy Practices a reference to that notice.
- (7) A statement of the ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization by stating either:
 - (a) That the covered entity may not condition treatment, payment, enrollment or eligibility for benefits on whether the individual signs the authorization when the prohibition on conditioning of authorizations applies; or,
 - (b) The consequences to the individual of a refusal to sign the authorization when the privacy rule permits the entity to condition treatment, enrollment in the health plan, or eligibility for benefits on failure to obtain the authorization.
- (8) A statement that information used or disclosed pursuant to the authorization may be subject to re-disclosure by the recipient and no longer be protected by the privacy rule;

- (9) Signature of the individual and date; and,
- (10) If the authorization is signed by a personal representative of the individual, a description of that personal representative's authority to act for the individual.

b. Additional Elements.

An authorization may contain elements or information in addition to the elements stated in Section VI.E.5.a, above, concerning "Required Elements", provided those additional elements or information are not inconsistent with the elements required by this Section VI.E.

c. Plain Language.

An authorization must be written in plain language.

d. Copy to Individual.

If CSCSO seeks an authorization from an individual for use or disclosure of protected health information, CSCSO will provide the individual with a copy of the signed authorization.

6. Compound Authorizations.

a. General Rule.

Except as stated in Section VI.E.6.b, below, an authorization for use or disclosure of protected health information may not be combined with any other document to create a compound authorization.

b. Exceptions.

Notwithstanding Section VI.E.6.a, above, an authorization for use or disclosure of protected health information may be combined with any other document to create a compound authorization in the following situations:

- (1) An authorization for the use or disclosure of protected health information created for a research study may be combined with any other type of written permission for the same research study, including another authorization for the use or disclosure of protected health information for such

- research or a consent to participate in such research;
- (2) An authorization, other than an authorization for a use or disclosure of psychotherapy notes, may be combined with any other authorization, except when CSCSO has conditioned the provision of treatment or payment under Section VI.E.6.b “Exceptions” (see, Page 21) of these privacy policies on the provision of one of the authorizations.

7. Revocation of an Authorization.

An individual has the right to revoke an authorization in writing, except to the extent CSCSO has taken action in reliance thereon.

A written revocation should be submitted to the Privacy Officer who will file the revocation his/her office.

8. Documentation.

The Home Supervisor, Program Coordinator, Sr. Program Coordinator, or Health Care Coordinator will document and retain any signed authorizations under this section in writing, or an electronic copy, for six (6) years from the date of its creation or the date when it was last in effect, whichever is later.

F. Uses and Disclosures Requiring an Opportunity for the Individual to Agree or to Object.

1. General Rule.

Members of CSCSO’s workforce may use or disclose protected health information without the individual’s written authorization for the purposes described in this Section VI.F provided:

- a. The individual is informed orally or in writing in advance of the use or disclosure; and,
- b. The individual has an opportunity to agree to or prohibit or restrict the disclosure in accordance with the requirements of this Section VI.F.

2. Persons Involved in the Individual’s Care; Notification.

a. General Rules.

- (1) **Those Involved in Care.** Members of CSCSO's workforce may, in accordance with Sections VI.F.2.b and VI.F.2.c, below, disclose to a family member, other relative, or a close personal friend of the individual, or to any other person identified by the individual, the protected health information directly relevant to that person's involvement with the individual's care or payment related to that individual's health care.
- (2) **Notification of Location, Condition, or Death.** Members of CSCSO's workforce may use or disclose protected health information to notify, or assist in the notification of (including identifying or locating) a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition or death. Any such use or disclosure must be in accordance with Section VI.F.2.b, VI.F.2.c, or VI.F.3, below.

b. When the Individual Is Present.

If the individual is present for, or otherwise available prior to, a use or disclosure to a person(s) involved in the individual's care and the individual has the capacity to make health care decisions, a member of CSCSO's workforce may use or disclose the protected health information if he or she:

- (1) Obtains the individual's agreement;
- (2) Provides the individual with the opportunity to object to the disclosure, and the individual does not express an objection; or,
- (3) Reasonably infers from the circumstances, based on the exercise of professional judgment, that the individual does not object to the disclosure.

c. When the Individual is Not Present.

- (1) **Incapacity; Emergency Circumstances.** If the individual is not present for, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the individual's incapacity or an emergency circumstance, a member of CSCSO's workforce may, in the exercise of professional judgment, determine whether

the disclosure is in the best interests of the individual and, if so, disclose only the protected health information that is directly relevant to the person's involvement with the individual's health care.

- (2) **Other Actions.** A member of CSCSO's workforce may use professional judgment and experience with common practice to make reasonable inferences of the individual's best interest in allowing a person to act on behalf of the individual to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of protected health information.

3. **Disaster Relief.**

A member of CSCSO's workforce may use or disclose protected health information to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, *e.g.*, the Red Cross, for the purpose of coordinating with such entities the uses and disclosures permitted by Section VI.F.2 "Persons Involved in the Individual's Care; Notification" (see, Page 22) concerning notification of location, condition or death. However, the requirements of Sections VI.F.2.b "When the Individual Is Present" (see, Page 23) and VI.F.2.c "When the Individual Is Not Present" (see, Page 23) of these privacy policies apply to those uses and disclosures to the extent that the CSCSO workforce member, in the exercise of professional judgment, determines that those requirements do not interfere with the ability to respond to the emergency circumstances.

G. **Uses and Disclosures for which an Authorization or an Opportunity to Agree or Object is Not Required.**

1. **General Rules.**

To the extent permitted by this Section VI.G, an authorized member of CSCSO's workforce may use or disclose protected health information without the authorization of the individual or the opportunity of the individual to agree or object, in the situations described in this Section VI.G.

When CSCSO is required by any of these situations to inform the individual of a use or disclosure permitted by this Section VI.G or when the individual may agree to a use or disclosure required by this Section VI.G, CSCSO's information and the individual's agreement may be given orally.

2. Uses and Disclosures Required by Law.

a. Informing the Privacy Officer.

Any member of CSCSO's workforce who receives a request, or who proposes, to use or disclose protected health information for a use or disclosure required by law must promptly deliver or otherwise communicate the request or proposal to the Privacy Officer prior to the use or disclosure being made. The Privacy Officer will then oversee the use or disclosure for compliance with these privacy policies. The use or disclosure should not occur until it has been approved by the Privacy Officer.

b. Permitted Uses and Disclosures.

CSCSO may use or disclose protected health information to the extent that the use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of the law.

CSCSO will meet the requirements of the following sections of these privacy policies, as applicable, for uses and disclosures required by law:

- (1) Section VI.G.4 "Uses and Disclosures About Victims of Abuse, Neglect or Domestic Violence"(see, Page 28);
- (2) Section VI.G.6 "Disclosures for Judicial and Administrative Proceedings" (see, Page 31); and,
- (3) Section VI.G.7 "Disclosures for Law Enforcement Purposes" (see, Page 34).

3. Uses and Disclosures for Public Health Activities.

a. Informing the Privacy Officer.

Any member of CSCSO's workforce who receives a request, or who proposes, to use or disclose protected health information for public health activities must promptly deliver or otherwise communicate the request or proposal to the Privacy Officer prior to the use or disclosure being made. The Privacy Officer will then oversee the use or disclosure for compliance with these privacy policies. The use or disclosure should not occur until it has been approved by the Privacy Officer.

b. Permitted Disclosures.

An authorized member of CSCSO's workforce may disclose protected health information for the public health activities and purposes described below:

- (1) A public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including but not limited to, the reporting of disease, injury and vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions; or, at the direction of the public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority;
- (2) A public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect;
- (3) A person subject to the jurisdiction of the United States Food and Drug Administration (FDA) with respect to an FDA-regulated product or activity for which that person has responsibility, for the purpose of activities related to the quality, safety or effectiveness of such FDA-regulated product or activity. Such purposes include:
 - (a) To collect or report adverse events (or similar activities with respect to food or dietary supplements), product defects or problems (including problems with the use or labeling of a product), or biological product deviations;
 - (b) To track FDA-regulated products;
 - (c) To enable product recalls, repairs, or replacement, or lookback (including locating and notifying individuals who have received products that have been recalled, withdrawn, or are the subject of lookback); or,
 - (d) To conduct post marketing surveillance.

- (4) A person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, if CSCSO or public health authority is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation; or
- (5) An employer, about an individual who is a member of the workforce of the employer, if:
 - (a) CSCSO provides health care to the individual at the request of the employer:
 - i) To conduct an evaluation relating to medical surveillance of the workplace; or,
 - ii) To evaluate whether the individual has a work-related illness or injury; or,
 - (b) The protected health information that is disclosed consists of findings concerning a work-related illness or injury or a work-related medical surveillance;
 - (c) The employer needs such findings in order to comply with its obligations under 29 CFR Parts 1904 through 1928 (concerning occupational safety and health), 30 CFR parts 50 through 90 (concerning mine safety and health), or similar state law, to record such illness or injury or to carry out responsibilities for workplace medical surveillance; and,
 - (d) CSCSO provides written notice to the individual that protected health information relating to the medical surveillance of the workplace and work-related illnesses and injuries is disclosed by the employer:
 - i) By giving a copy of the notice to the individual at the time the health care is provided; or
 - ii) If the health care is provided on the work site of the employer, by posting the notice in

a prominent place at the location where the health care is provided.

4. Uses and Disclosures About Victims of Abuse, Neglect or Domestic Violence.

a. Delivery to Privacy Officer.

Any member of CSCSO's workforce who receives a request, or who proposes, to use or disclose protected health information about a victim of abuse, neglect or domestic violence must promptly deliver or otherwise communicate the request or proposal to the Privacy Officer prior to the use or disclosure being made. The Privacy Officer will then oversee the use or disclosure for compliance with these privacy policies. The use or disclosure should not occur until it has been approved by the Privacy Officer.

b. General Rule.

Except for reports of child abuse or neglect that are permitted by Section VI.G.3.b.(2) "Permitted Disclosures" (see, Page 26) of these privacy policies, an authorized member of CSCSO's workforce may disclose protected health information about an individual that workforce member reasonably believes to be a victim of abuse, neglect, or domestic violence to a government authority, including a social service or protective services agency, authorized by law to receive reports of such abuse, neglect or domestic violence:

- (1) To the extent the disclosure is required by law and the disclosure complies with and is limited to the relevant requirements of that law;
- (2) If the individual agrees to the disclosure; or,
- (3) To the extent the disclosure is expressly authorized by statute or regulation and:
 - (a) The CSCSO workforce member, in the exercise of professional judgment, believes the disclosure is necessary to prevent serious harm to the individual or other potential victim; or,
 - (b) If the individual is unable to agree because of incapacity, a law enforcement or other public

official authorized to receive the report represents that:

- i) The protected health information for which disclosure is sought is not intended to be used against the individual; and,
- ii) An immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

c. Informing the Individual.

If a member of CSCSO's workforce makes a disclosure permitted by VI.G.4.b "General Rule", above, the Privacy Officer shall promptly inform the individual that such a report has been or will be made, except if:

- (1) The Privacy Officer, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm; or
- (2) The Privacy Officer would be informing a personal representative, and he or she reasonably believes the personal representative is responsible for the abuse, neglect or other injury, and that informing that person would not be in the best interests of the individual as determined by CSCSO, in the exercise of professional judgment.

5. Uses and Disclosures for Health Oversight Activities.

a. Delivery to Privacy Officer.

Any member of CSCSO's workforce who receives a request, or who proposes, to use or disclose protected health information for purposes of a health oversight activity must promptly deliver or otherwise communicate the request or proposal to the Privacy Officer prior to the use or disclosure being made. The Privacy Officer will then oversee the use or disclosure for compliance with these privacy policies. The use or disclosure should not occur until it has been approved by the Privacy Officer.

b. General Rule.

An authorized member of CSCSO’s workforce may disclose protected health information to a health oversight agency, *e.g.*, state department of health, CMS, for oversight activities authorized by law, including: audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or other actions; or, other activities necessary for appropriate oversight of:

- (1) The health care system;
- (2) Government benefit programs for which health information is relevant to beneficiary eligibility;
- (3) Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or,
- (4) Entities subject to civil rights laws for which health information is necessary for determining compliance.

c. Exceptions.

For purposes of the disclosures permitted by Section VI.G.5.b “General Rule”, above, a health oversight activity does not include an investigation or other activity in which the individual is the subject of the investigation or activity and such investigation or other activity does not arise out of and is not directly related to:

- (1) The receipt of health care;
- (2) A claim for public benefits related to health; or,
- (3) Qualification for, or receipt of, public benefits or services when an individual’s health is integral to the claim for public benefits or services.

d. Joint Activities or Investigations.

Notwithstanding the exceptions stated in Section VI.G.5.c, above, if a health oversight activity or investigation is conducted in conjunction with an oversight activity or investigation relating to a claim for public benefits not related to health, the joint activity or investigation is considered a health oversight activity for purposes of this section.

6. Disclosures for Judicial and Administrative Proceedings.

a. Delivery to Privacy Officer.

Any member of CSCSO's workforce who receives an order of a court or administrative tribunal or a subpoena, discovery request, or other lawful process must promptly deliver or otherwise communicate the document to the Privacy Officer prior to the disclosure being made. The Privacy Officer will then oversee the disclosure for compliance with these privacy policies. The disclosure should not occur until it has been approved by the Privacy Officer.

b. General Rules.

CSCSO will disclose protected health information in the course of any judicial or administrative proceeding:

- (1) In response to an order of a court or administrative tribunal, provided CSCSO will disclose only the protected health information expressly authorized by the order; or,
- (2) In response to a subpoena, discovery request, or other lawful process, that is not accompanied by an order of a court or administrative tribunal, if:
 - (a) CSCSO receives satisfactory assurance, as described below, from the party seeking the information that reasonable efforts have been made by that party to ensure that the individual who is the subject of the protected health information that has been requested has been given notice of the request; or,
 - (b) CSCSO receives satisfactory assurance, as described below, from the party seeking the information that reasonable efforts have been made by that party to secure a qualified protective order that meets the requirements stated below.
 - (c) Notwithstanding (a) and (b), above, CSCSO may disclose protected health information in response to a subpoena, discovery request or other lawful process that is not accompanied by an order of the

court or administrative tribunal, without satisfactory assurance, if CSCSO, itself:

- i) Makes reasonable efforts to provide notice to the individual sufficient to meet the requirements stated below for satisfactory assurance of such a notice; or,
- ii) Seeks a qualified protective order sufficient to meet the requirements stated below for a qualified protective order.

c. Satisfactory Assurance.

(1) That Individual Has Received Notice. CSCSO will be considered to have received “satisfactory assurance” from a party seeking protected health information that the individual has received notice if CSCSO receives from that party a written statement and accompanying documentation demonstrating that:

- (a) The party requesting the information has made a good faith attempt to provide written notice to the individual (or, if the individual’s location is unknown, to mail a notice to the individual’s last known address);
- (b) The notice included sufficient information about the litigation or proceeding in which the protected health information is requested to permit the individual to raise an objection to the court or administrative tribunal; and,
- (c) The time for the individual to raise objections to the court or administrative tribunal has elapsed, and:
 - i) No objections were filed; or,
 - ii) All objections filed by the individual have been resolved by the court or the administrative tribunal and the disclosures being sought are consistent with that resolution.

(2) That Qualified Protective Order Sought. CSCSO will be

considered to have received “satisfactory assurance” from a party seeking protected health information that a qualified protective order has been sought if CSCSO receives from that party a written statement and accompanying documentation demonstrating that:

- (a) The parties to the dispute giving rise to the request for information have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or,
- (b) The party seeking the protected health information has requested a qualified protective order from that court or administrative tribunal.

(3) Meaning of “Qualified Protective Order”. A “qualified protective order” means an order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that:

- (a) Prohibits the parties from using or disclosing the protected health information for any purpose other than the litigation or proceeding for which the information was requested; and,
- (b) Requires the return to CSCSO or destruction of the protected health information (including all copies made) at the end of the litigation or proceeding.

d. Not Limitation on Other Uses and Disclosures.

The provisions of this section dealing with disclosures for judicial and administrative proceedings do not supersede other provisions of these privacy policies that otherwise permit or restrict uses of disclosures of protected health information.

7. Disclosures for Law Enforcement Purposes.

a. Delivery to Privacy Officer.

Any member of CSCSO's workforce who receives a request, or proposes, to disclose protected health information for law enforcement purposes must promptly deliver or otherwise communicate the request or proposal to the Privacy Officer prior to the disclosure being made. The Privacy Officer will then oversee the use or disclosure for compliance with these privacy policies. The use or disclosure should not occur until it has been approved by the Privacy Officer.

b. Pursuant to Process and As Otherwise Required by Law.

An authorized member of CSCSO's workforce may disclose protected health information:

- (1) As required by law including laws that require the reporting of certain types of wounds or other physical injuries, except:
 - (a) For laws concerning a public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect (see, Section VI.G.3.b.(1) "Permitted Disclosures" on Page 26 of these privacy policies); or,
 - (b) To the extent the disclosure is pursuant to a mandatory reporting law concerning reporting of abuse, neglect, or domestic violence and the disclosure complies with and is limited to the relevant requirements of that law (see, Section VI.G.4.b.(1) on Page 28 of these privacy policies).
- (2) In compliance with and as limited by relevant requirements of:
 - (a) A court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer;
 - (b) A grand jury subpoena; or,
 - (c) An administrative request, including an administrative subpoena or summons, a civil or an authorized

investigative demand, or similar process authorized under law, provided that:

- i) The information sought is relevant and material to a legitimate law enforcement inquiry;
- ii) The request is specific and limited in scope to the extent reasonably practical in light of the purpose for which the information is sought; and,
- iii) De-identified information could not reasonably be used.

(For verification of an administrative request see Section VI.K.3.a, “Conditions on Disclosures” on Page 49 of these privacy policies.)

c. Limited Information for Identification and Location Purposes.

Except for disclosures required by law as permitted by VI.G.7.b, above, (see, Page 34) an authorized member of CSCSO’s workforce may disclose protected health information in response to a law enforcement official’s request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, provided that:

- (1) CSCSO may disclose only the following information:
 - (a) Name and address;
 - (b) Date and place of birth;
 - (c) Social security number;
 - (d) ABO blood type and rh factor;
 - (e) Type of injury;
 - (f) Date and time of treatment;
 - (g) Date and time of death, if applicable; and,
 - (h) A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence of absence of facial hair (beard or moustache), scars, and tattoos.
- (2) Except as stated in (1), above, a member of CSCSO’s workforce may not disclose for the purposes of identification or location under this section any protected

health information related to the individual's DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue.

d. Victims of a Crime.

Except for disclosures required by law as permitted by VI.G.7.b, above, (see, Page 34) an authorized member of CSCSO's workforce may disclose protected health information in response to a law enforcement official's request for such information about an individual who is or is suspected to be a victim of a crime, other than disclosures that are subject to Section VI.G.7.b and Section VI.G.7.c, if:

- (1) The individual agrees to the disclosure; or,
- (2) CSCSO is unable to obtain the individual's agreement because of incapacity or other emergency circumstance, provided that:
 - (a) The law enforcement official represents that such information is needed to determine whether a violation of law by a person other than the victim has occurred, and such information is not intended to be used against the victim;
 - (b) The law enforcement official represents that immediate law enforcement activity that depends on the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure; and,
 - (c) The disclosure is in the best interests of the individual as determined by CSCSO, in the exercise of professional judgment.

e. Decedents.

An authorized member of CSCSO's workforce may disclose protected health information about an individual who has died to a law enforcement official for the purpose of alerting law enforcement of the death of the individual if CSCSO has a suspicion that such death may have resulted from criminal conduct.

f. Crime on the Premises.

An authorized member of CSCSO's may disclose to a law enforcement official protected health information that he or she believes in good faith constitutes evidence of criminal conduct that occurred on the premises of CSCSO.

g. Reporting Crime in Emergencies.

If CSCSO is providing emergency health care in response to a medical emergency, other than on the premises of CSCSO, an authorized member of CSCSO's workforce may disclose protected health information to a law enforcement official if such disclosure appears necessary to alert law enforcement to:

- (1) The commission and nature of a crime;
- (2) The location of such crime or of the victim(s) of such crime; and,
- (3) The identity, description, and location of the perpetrator of the crime.

If the member of CSCSO's workforce believes the medical emergency is the result of abuse, neglect, or domestic violence of the individual in need of emergency health care, the preceding does not apply and any disclosure to a law enforcement official for law enforcement purposes is subject to Section VI.G.7.c (see, Page 35) of these privacy policies.

8. Uses and Disclosures about Decedents.

a. Delivery to Privacy Officer.

Any member of CSCSO's workforce who receives a request, or proposes to use or disclose protected health information to a coroner, medical examiner, or funeral director must promptly deliver or otherwise communicate the request or proposal to the Privacy Officer prior to the use or disclosure being made. The Privacy Officer will then oversee the use or disclosure for compliance with these privacy policies. The use or disclosure may not occur until it has been approved by the Privacy Officer.

b. Coroners and Medical Examiners.

An authorized member of CSCSO's workforce may disclose

protected health information to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law.

c. Funeral Directors.

An authorized member of CSCSO's workforce may disclose protected health information to funeral directors consistent with applicable law, as necessary to carry out their duties with respect to the decedent. If necessary for funeral directors to carry out their duties, CSCSO may disclose the protected health information prior to, and in reasonable anticipation of, the individual's death.

9. Uses and Disclosures for Cadaveric Organ, Eye or Tissue Donation.

a. Delivery to Privacy Officer.

Any member of CSCSO's workforce who receives a request, or proposes, to use or disclose protected health information for purposes of cadaveric organ, eye or tissue donation must promptly deliver or otherwise communicate the request or proposal to the Privacy Officer prior to the use or disclosure being made. The Privacy Officer will then oversee the use or disclosure for compliance with these privacy policies. The use or disclosure may not occur until it has been approved by the Privacy Officer.

b. Permitted Uses and Disclosures.

An authorized member of CSCSO's workforce may use or disclose protected health information to organ procurement organizations or other entities engaged in the procurement, banking or transplantation of cadaveric organs, eyes or tissue for the purpose of facilitating organ, eye or tissue donation and transplantation.

10. Uses and Disclosures to Avert a Serious Threat to Health or Safety.

a. Delivery to Privacy Officer.

Any member of CSCSO's workforce who receives a request, or proposes, to use or disclose protected health information to avert a serious threat to health or safety must promptly deliver or otherwise communicate the request or proposal to the Privacy Officer prior to the use or disclosure being made. The Privacy Officer will then oversee the use or disclosure for compliance with these privacy policies. The use or disclosure may not occur until it has been approved by the Privacy Officer.

b. Permitted Uses and Disclosures.

An authorized member of CSCSO's workforce may, consistent with applicable law and standards of ethical conduct, use or disclose protected health information, if the member of CSCSO's workforce, in good faith, believes the use or disclosure:

(1) Serious and Imminent Threat.

- (a) Is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public; and,
- (b) Is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat.

(2) Law Enforcement. Is necessary for law enforcement authorities to identify or apprehend an individual:

- (a) Because of a statement by an individual admitting participation in a violent crime that CSCSO reasonably believes may have caused serious physical harm to the victim; or,
- (b) Where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody.

c. Uses and Disclosures Not Permitted.

A use or disclosure pursuant to Section VI.G.10.b.(2)(a), above, concerning a statement of an individual may not be made if the information described in that section is learned by CSCSO:

- (1) In the course of treatment to affect the propensity to commit the criminal conduct that is that basis for the disclosure under that section, or counseling or therapy; or,
- (2) Through a request by the individual to initiate or to be referred for the treatment, counseling, or therapy described in Section VI.G.10.b.(2)(a), above.

A disclosure made pursuant to Section VI.G.10.b.(2)(a), above,

shall contain only the statement described in that section and the protected health information described in Section VI.G.7.c.(1) “Limited Information for Identification and Location Purposes” (see, Page 35) of these privacy policies.

11. Uses and Disclosures for Specialized Government Functions.

a. Delivery to Privacy Officer.

Any member of CSCSO’s workforce who receives a request, or proposes to use or disclose protected health information for purposes of a specialized government function described in this Section VI.G.11 must promptly deliver or otherwise communicate the request or proposal to the Privacy Officer prior to the use or disclosure being made. The Privacy Officer will then oversee the use or disclosure for compliance with these privacy policies. The use or disclosure may not occur until it has been approved by the Privacy Officer.

b. Military and Veterans Activities.

(1) Armed Forces Personnel. An authorized member of CSCSO’s workforce may use and disclose the protected health information of individuals who are Armed Forces personnel for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission, if the appropriate military authority has published by notice in the *Federal Register* the following information:

- (a) Appropriate military command authorities; and,
- (b) The purposes for which the protected health information may be used or disclosed.

(2) Foreign Military Personnel. An authorized member of CSCSO’s workforce may use and disclose the protected health information of individuals who are foreign military personnel to their appropriate foreign military authority for the same purposes for which uses and disclosures are permitted for Armed Forces personnel under the notice published in the *Federal Register*.

c. National Security and Intelligence Activities.

An authorized member of CSCSO's workforce may disclose protected health information to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act, 50 U.S.C. 401 *et seq* and implementing authority, *e.g.*, Executive Order 12333.

d. Protective Services for the President and Others.

An authorized member of CSCSO's workforce may disclose protected health information to authorized federal officials for the provision of protective services to the President of the United States or other persons authorized by 18 U.S.C. 3056, or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or to for the conduct of investigations authorized by 18 U.S.C. 871 and 879.

e. Correctional Institutions and Other Law Enforcement Custodial Situations.

(1) Permitted Disclosures. An authorized member of CSCSO's workforce may disclose to a correctional institution or a law enforcement official having lawful custody of an inmate or other individual protected health information about such inmate or individual, if the correctional institution or such law enforcement official represents that such protected health information is necessary for:

- (a) The provision of health care to such individuals;
- (b) The health and safety of such individual or other inmates;
- (c) The health and safety of the officers or employees of or others at the correctional institution;
- (d) The health and safety of such individuals and officers or other persons responsible for the transporting of inmates or their transfer from one institution, facility, or setting to another;
- (e) Law enforcement on the premises of the correctional institution; and,

(f) The administration and maintenance of the safety, security, and good order of the correctional institution.

(2) **No Application After Release.** For purposes of this provision, an individual is no longer an inmate when released on parole, probation, supervised release, or otherwise is no longer in lawful custody.

12. Disclosures for Workers' Compensation.

a. Delivery to Privacy Officer.

Unless the use or disclosure has previously been approved by the Privacy Officer, a member of CSCSO's workforce who receives a request, or proposes, to disclose protected health information to comply with laws relating to workers compensation or other similar programs, must promptly deliver or otherwise communicate the request or proposal to the Privacy Officer prior to the disclosure being made. The Privacy Officer will then oversee the use or disclosure for compliance with these privacy policies. The use or disclosure should not occur until it has been approved by the Privacy Officer.

b. Permitted Disclosures.

An authorized member of CSCSO's workforce may disclose protected health information as authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs, established by law, that provide benefits for work-related injuries or illnesses without regard to fault.

13. Disclosure to the Secretary of Health and Human Services.

a. Delivery to Privacy Officer.

Any member of CSCSO's workforce who receives a request, or proposes to disclose protected health information to the Secretary of Health and Human Services must promptly deliver or otherwise communicate the request or proposal to the Privacy Officer prior to the disclosure being made. The Privacy Officer will then oversee the disclosure for compliance with these privacy policies. The use or disclosure should not occur until it has been approved by the Privacy Officer.

b. Permitted Disclosures.

Acting through its Privacy Officer, CSCSO will permit access by the Secretary of Health and Human Services during normal business hours to its facilities, books, records, accounts and other sources of information, including protected health information, that are pertinent to ascertaining compliance with the applicable requirements of the HIPAA privacy rule. If the Secretary of Health and Human Services determines that exigent circumstances exist, such as when documents may be hidden or destroyed, CSCSO will permit access by the Secretary of Health and Human Services at any time and without notice.

If any information required of CSCSO under this section is in the exclusive possession of any other agency, institution, or person and that other agency, institution or person fails or refuses to furnish the information, the Privacy Officer will so certify and set forth what efforts CSCSO has made to obtain the information.

14. Disclosures by Whistleblowers.

A member of CSCSO's workforce or a business associate may disclose protected health information, provided that:

- a. The workforce member or business associate believes in good faith that CSCSO has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services or conditions provided by CSCSO potentially endangers one or more individuals, workers, or the public; and,
- b. The disclosure is to:
 - (1) A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of CSCSO or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by CSCSO; or,
 - (2) An attorney retained by or on behalf of the workforce member or business associate for the purpose of determining the legal options of the workforce member or business associate with regard to the conduct described in Section a., above.

The disclosure does not need to be approved by the Privacy Officer before it is made.

15. Disclosures by Workforce Members Who are Victims of a Crime.

A workforce member who is the victim of a criminal act may disclose protected health information to a law enforcement official, provided that:

- a. The protected health information disclosed is about the suspected perpetrator of the criminal act; and,
- b. The protected health information disclosed is limited to the following information:
 - (1) Name and address;
 - (2) Date and place of birth;
 - (3) Social security number;
 - (4) ABO blood type and Rh factor;
 - (5) Type of injury;
 - (6) Date and time of treatment;
 - (7) Date and time of death, if applicable; and,
 - (8) A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence of absence of facial hair (beard or moustache), scars, and tattoos.

The disclosure does not need to be approved by the Privacy Officer before it is made.

16. Disclosures to Business Associates.

a. Delivery to Privacy Officer.

Unless the use or disclosure has previously been approved by the Privacy Officer, any member of CSCSO's workforce who receives a request, or proposes to disclose protected health information to a business associate of CSCSO must promptly deliver or otherwise communicate the request or proposal to the Privacy Officer prior to the disclosure being made. The Privacy Officer will then oversee the use or disclosure for compliance with these privacy policies. The use or disclosure may not occur until it has been approved by the Privacy Officer.

b. Permitted Disclosures.

Authorized members of CSCSO’s workforce may disclose protected health information to a business associate and may allow a business associate to create or receive protected health information on CSCSO’s behalf, if CSCSO has a written contract with the business associate that meets the requirements of the HIPAA privacy rule.

H. Uses and Disclosures for Marketing.

1. General Rule.

Except as stated in section VI.H.2, below, a member of CSCSO’s workforce may not use protected health information for marketing without an authorization that meets the applicable requirements of Section VI.E (see, Page 17) of these privacy policies, except as stated in this Section VI.H.

Any use of protected health information for marketing without an authorization must be approved in advance by the Privacy Officer.

2. Exceptions.

An authorization does not need to be obtained if CSCSO uses or discloses protected health information to make a marketing communication to an individual that is in the form of:

- a. A face-to-face communication made by CSCSO to an individual;
or,
- b. A promotional gift of nominal value provided by CSCSO.

If the marketing involves direct or indirect remuneration to CSCSO from a third party, the authorization must state that such remuneration is involved.

3. “Marketing” Defined.

“Marketing” means:

- a. To make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service, unless the communication is made:
 - (1) To describe a health-related product or service that is provided by the covered entity making the communication;
or,

- (2) For treatment of the individual; or,
 - (3) For case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual.
- b. An arrangement between a covered entity and any other entity whereby the covered entity discloses protected health information to the other entity, in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about its own product or service that encourages recipients of the communication to purchase that product or service.

I. Uses and Disclosures for Fundraising.

1. General Rule.

An authorized member of CSCSO's workforce may use, or disclose to a business associate, the following protected health information for the purpose of raising funds for its own benefit, without an authorization meeting the requirements of Section VI.E "Uses and Disclosures for Which an Authorization is Required" (see, Page 17) of these privacy policies:

- a. Demographic information relating to an individual; and,
- b. Dates of health care provided to an individual.

Any use of protected health information for the purpose of raising funds for CSCSO's benefit without an authorization must be approved in advance by the Privacy Officer.

2. Opting Out.

Any fundraising materials CSCSO sends to an individual must include a description of how the individual may opt out of receiving any further fundraising communications.

CSCSO must make reasonable efforts to ensure that individuals who decide to opt out of receiving future marketing communications are not sent future communications.

J. Limited Data Set.

1. General Rule.

CSCSO may use or disclose a limited data set that meets the requirements of Section VI.J.3 “Limited Data Set Defined”, below, if CSCSO enters into a “data use agreement” with the limited data set recipient. Prior to CSCSO using or disclosing any protected health information as part of a “limited data set”, both the limited data set and the data use agreement must be approved by the Privacy Officer as meeting the requirements of this Section VI.J.

2. Permitted Uses.

- a. A limited data set may be used and disclosed only for the purposes of research, public health, or health care operations.
- b. CSCSO may use protected health information to create a limited data set or disclose protected health information to a business associate of CSCSO for that purpose, whether or not the limited data set is to be used by CSCSO.

3. “Limited Data Set” Defined.

A “limited data set” is protected health information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:

- (i) Names;
- (ii) Postal address information, other than town or city, State, and zip code;
- (iii) Telephone numbers;
- (iv) Fax numbers;
- (v) Electronic mail addresses;
- (vi) Social security numbers;
- (vii) Medical record numbers;
- (viii) Health plan beneficiary numbers;
- (ix) Account numbers;
- (x) Certificate/license numbers;
- (xi) Vehicle identifiers and serial numbers, including license plate numbers;
- (xii) Device identifiers and serial numbers;
- (xiii) Web Universal Resources Locators (URLs);
- (xiv) Internet Protocol (IP) address numbers;
- (xv) Biometric identifiers, including finger and voice prints; and

(xvi) Full face photographic images and any comparable images.

4. Data Use Agreement.

A data use agreement between CSCSO and the limited data set recipient must:

- a. Establish the permitted uses and disclosures of the limited data set by the limited data set recipient consistent with the permitted uses stated above. The data use agreement may not authorize the limited data set recipient to use or further disclose the information in a manner that would violate the requirements of these policies or the HIPAA privacy rule if done by CSCSO;
- b. Establish who is permitted to use or receive the limited data set; and,
- c. Provide that the limited data set recipient will:
 - (1) Not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law;
 - (2) Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement;
 - (3) Report to the covered entity any use or disclosure of the information not provided for by its data use agreement of which it becomes aware;
 - (4) Ensure that any agents, including a subcontractor, to whom it provides the limited data set agrees to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and,
 - (5) Not identify the information or contact the individuals.

K. Verification of Identity and Authority.

1. General Rule.

Prior to any disclosure of protected health information, the authorized member of CSCSO's workforce who is making the disclosure must:

- a. Except with respect to disclosures under VI.F, “Uses and Disclosures Requiring an Opportunity for the Individual to Agree or to Object” (see, Page 22) of these privacy policies, verify the identity of a person requesting protected health information and the authority of that person to have access to protected health information under these privacy policies, if the identity of that person is not known to CSCSO; and,
- b. Obtain any documentation, statements, or representations, whether oral or written, from the person requesting the protected health information when such documentation, statement, or representation is a condition of the disclosure under these privacy policies.

2. Personal Representatives.

Unless the person and his or her authority is known to CSCSO, the authorized member of CSCSO’s workforce who is making a disclosure to an individual’s personal representative shall verify the person’s identity by way of a government issued document with a picture (e.g., a driver’s license, passport) and verify the person’s authority (e.g., requiring a copy of a power of attorney, asking questions to establish relationship to a child.)

3. Conditions on Disclosures.

If a disclosure is conditioned by these privacy policies on particular documentation, statements, or representations from the person requesting the protected health information, the authorized member of CSCSO’s workforce who is making the disclosure may rely, if such reliance is reasonable under the circumstances, on documentation, statements, or representations that, on their face, meet the applicable requirements.

In this regard:

- a. The conditions in Section VI.G.7.b.(2)(c) under “Disclosures for Law Enforcement Purposes” (see, Page 34) of these privacy policies may be satisfied by the administrative subpoena or similar process or by a separate written statement that, on its face, demonstrates that the applicable requirements have been met.

4. Identity of Public Officials.

CSCSO may rely, if such reliance is reasonable under the circumstances, on any of the following to verify identity when the disclosure of protected health information is to a public official or a person acting on behalf of a public official:

- a. If the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status;
- b. If the request is made in writing, the request is on the appropriate government letterhead; or,
- c. 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, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.

5. Authority of Public Officials.

CSCSO may rely, if such reliance is reasonable under the circumstances, on any of the following to verify authority when the disclosure of protected health information is to a public official or a person acting on behalf of a public official:

- a. A written statement of the legal authority under which the information is requested, or, if a written statement would be impractical, an oral statement of such legal authority;
- b. 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 is presumed to constitute legal authority.

6. Exercise of Professional Judgment.

The verification requirements of this section are met if a member of CSCSO's workforce relies on the exercise of professional judgment in making a use or disclosure in accordance with Section VI.F, "Uses or Disclosures Requiring an Opportunity for the Individual to Agree or Object" (see, Page 22) of these privacy policies or acts on a good faith belief in making a disclosure in accordance with Section VI.G.10, "Uses or Disclosures to Avert a Serious Threat to Health or Safety" (see, Page 38) of these privacy policies.

L. Prior Authorizations.

1. General Rule.

Notwithstanding other sections of these privacy policies, CSCSO may use or disclose protected health information, consistent with Section VI.L.2, below, pursuant to an authorization or other express legal permission obtained from an individual permitting the use or disclosure of protected health information, informed consent of the individual to participate in research, or a waiver of informed by an Institutional Review Board.

2. Effect of Prior Authorization for Purposes Other Than Research.

Notwithstanding any provisions of Section VI.E “Uses and Disclosures for Which an Authorization is Required” of these privacy policies (see Page 17), CSCSO may use or disclose protected health information that it created or received prior to April 14, 2003, pursuant to an authorization or other express legal permission obtained from an individual prior to April 14, 2003, provided the authorization or other express legal permission specifically permits such use or disclosure and there is no agreed-to restriction in accordance with Section VII.A.1 “Right to Request Privacy Protection” of these privacy policies (see Page 51).

VII. RIGHTS OF INDIVIDUALS.

A. Right to Request Privacy Protection.

1. Restriction of Uses and Disclosures.

a. Generally.

CSCSO will permit an individual to request that CSCSO restrict:

- (1) Uses and disclosures of protected health information about the individual to carry out treatment, payment or health care operations; and,
- (2) Disclosures permitted under Section VI.F.2, “Persons Involved in the Individual’s Care; Notification” (see, Page 22) of these privacy policies, for involvement in the individual’s care and notification purposes.

Whether or not CSCSO will agree to the restriction will be determined by the Privacy Officer. If a restriction is agreed to, a written or electronic record of that restriction shall be retained by CSCSO

for six years from the date of its creation or the date when it was last in effect, whichever is later.

If CSCSO agrees to a restriction, the protected health information shall not be used or disclosed in violation of such restriction, except

that, if the individual who requested the restriction is in need of emergency treatment and the restricted protected health information is needed to provide the emergency treatment, the restricted protected health information may be used by CSCSO, or may be disclosed by an authorized member of CSCSO's workforce to a health care provider, to provide such treatment to the individual. If the information is disclosed to a health care provider for emergency treatment, the member of CSCSO's workforce making the disclosure shall request that health care provider not further use or disclose the information.

A restriction agreed to by CSCSO under this Section VII.A.1.a is not effective to prevent uses or disclosures:

- (a) To the individual when requested by the individual pursuant to the individual's right of access to the information (see, Section VII.B, "Right of Access" on Page 53 of these privacy policies);
- (b) When the use or disclosure does not require an authorization or opportunity to agree or object is not required (see, Section VI.G, "Uses and Disclosures for which an Authorization or an Opportunity to Agree or Disagree is Not Required" on Page 24 of these privacy policies).

b. Termination of Restriction.

CSCSO may terminate its agreement to a restriction under this Section VII.A.1, if:

- (1) The individual agrees to or requests the termination in writing;
- (2) The individual orally agrees to the termination and the oral agreement is documented; or,
- (3) CSCSO informs the individual that it is terminating its agreement to the restriction, except that such termination shall be effective only with respect to protected health

information created or received after CSCSO has so informed the individual.

2. Restriction on Means and Location of Communications.

a. Generally.

CSCSO shall permit individuals to request and, subject to the conditions stated below, shall accommodate reasonable requests by individuals to receive communications of protected health information from CSCSO by alternative means or at alternative locations.

The request by the individual to receive communications by alternative means or at alternative locations must be in writing.

b. Conditions.

CSCSO's accommodation of such requests shall be conditioned on:

- (a) When appropriate, information as to how payment, if any, will be handled; and,
- (b) Specification by the individual of an alternative address or other method of contact.

CSCSO shall not require an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis.

B. Right of Access.

1. Generally.

Except when access is denied under Section VII.B.5, "Denial of Access" (see, Page 56) of these privacy policies, an individual shall have a right of access to inspect and obtain a copy of protected health information about the individual for as long as the protected health information is maintained in that record set except for:

- a. Psychotherapy notes;
- b. Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; and

2. Request for Access.

The individual's request for access must be submitted in writing to the Home Supervisor, Program Coordinator, Senior Program Coordinator, or Health Care Coordinator.

3. Action on Request for Access.

a. Time Limits for Action.

The HS, PC, SPC, or Health Care Coordinator shall act on a request for access no later than thirty (30) calendar days after CSCSO's receipt of the request. However, if the request for access is for protected health information that is not maintained or accessible to CSCSO on-site, the HS, PC, SPC, or HCC shall act on the request for access no later than sixty (60) calendar days after CSCSO's receipt of the request.

If the HS, PC, SPC, or HCC is unable to take an action on the request within the applicable time required by the preceding paragraph, the HS, PC, SPC, or HCC may extend the time for the action by no more than thirty (30) calendar days, provided:

- (1) Within the applicable time required by the preceding paragraph, the HS, PC, SPC, or HCC shall provide the individual with a written statement of the reason(s) for the delay and the date by which CSCSO will complete its action on the request; and,
- (2) Only one such extension shall be permitted on a request for access.

b. Inform Individual of Action on Request.

If the request is granted, in whole or in part, the HS, PC, SPC, or HCC shall inform the individual of the acceptance of the request and provide the access requested in accordance with Section VII.B.4, below.

If the request is denied, in whole or in part, the HS, PC, SPC, or HCC shall provide the individual with a written denial, in accordance with Section VII.B.6.b, "Actions if Access is Denied" (see, Page 67), of these privacy policies.

4. Providing Access.

a. Access.

If the individual is granted access, in whole or in part, to protected health information, CSCSO shall provide the access requested by the individual, including inspection and obtaining a copy, or both, of the protected health information about the individual in designated record sets. If the same protected health information that is the subject of a request for access is maintained in more than one designated record set or at more than one location, the protected health information will only be produced once in response to a request for access.

b. Form and Format.

The protected health information will be provided to the individual in the form or format requested by the individual, if it is readily producible in that form or format. If it is not readily producible in that form or format, it shall be provided in a readable hard copy form or such other form or format as agreed to by the HS, PC, SPC, or HCC and the individual.

c. Summary In Lieu of Access.

The individual may be provided a summary of the protected health information requested, in lieu of providing access to the protected health information, or may be provided an explanation of the protected health information to which access has been provided, if:

- (1) The individual agrees in advance to such a summary or explanation; and,
- (2) The individual agrees in advance to the fees imposed, if any, by CSCSO for such summary or explanation.

d. Time and Manner of Access.

Access shall be provided in a timely manner as stated in Section VII.B.3.a, "Action on Request for Access" (see, Page 54), of these privacy policies, including arranging with the individual for a convenient time and place to inspect or obtain a copy of the protected health information, or mailing the copy to the individual at the individual's request. The HS, PC, SPC, or HCC may discuss the scope, format and other aspects of the request for access with the individual as necessary to facilitate the timely provision of

access.

e. Fees.

If the individual requests a copy of the protected health information, or agrees to a summary or explanation of such information, CSCSO shall impose charges as set forth in Appendix E to these privacy policies. At any time and upon his/her discretion, the Privacy Officer may waive the fee.

5. Denial of Access.

a. Unreviewable Grounds for Denial.

CSCSO may deny an individual access without providing the individual an opportunity for review, in any the following circumstances:

- (1) Information Is Exempted.** The protected health information is exempted from the right of access as stated in Section VII.B.1, “Generally” (see, Page 53), of these privacy policies.
- (2) Inmates.** When CSCSO is acting under the direction of a correctional institution, CSCSO may deny, in whole or in part, an inmate’s request to obtain a copy of protected health information, if obtaining such copy would jeopardize the health, safety, security, custody, or rehabilitation of the individual or of other inmates, or the safety of any officer, employee, or other person at the correctional institution or reasonable for the transporting of the inmate.
- (3) Information Obtained From Others.** An individual’s access may be denied if the protected health information 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.

b. Reviewable Grounds for Denial.

CSCSO may deny an individual access, provided that the individual is given a right to have the denial reviewed as stated in Section VII.B.6.c, “Review of Denial” (see, Page 58), of these privacy policies, in any the following circumstances:

- (1) **Endangerment.** 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 individual or another person;
- (2) **Reference to Another Person.** The protected health information 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
- (3) **Personal Representative.** The request for access is made by the 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 individual or another person.

6. Actions if Access is Denied.

If an individual's access to protected health information is denied, in whole or in part, CSCSO shall comply with the following:

a. Making Other Information Accessible.

CSCSO shall, to the extent possible, give the individual access to any other protected health information requested, after excluding the protected health information as which CSCSO had the ground to deny access.

b. Written Denial.

The Privacy Officer shall provide a written denial to the individual within the applicable time period stated in Section VII.B.6.c, "Review of Denial" (see, Page 58), of these privacy policies. The denial shall contain:

- (1) The basis for the denial;
- (2) If applicable, a statement of the individual's review rights, including a description of how the individual may exercise

such review rights;

- (3) A description of how the individual may complain pursuant to CSCSO's complaint procedures or to the Secretary of Health and Human Resources, including the name or title, and the telephone number of the CSCSO contact person or office designated to receive complaints.
- (4) If CSCSO does not maintain the protected health information that is the subject of the individual's request for access, and CSCSO knows where the requested information is maintained, a statement informing the individual where to direct the request for access.

c. Review of Denial.

If access is denied on a ground permitted under Section VII.B.5.b, "Reviewable Grounds for Denial" (see, Page 56) of these privacy policies, above, the individual shall have the right to have the denial reviewed by a licensed health care professional who is designated by the Privacy Officer to act as a reviewing official and who did not participate in the original decision to deny.

The individual's request for review shall be promptly referred to that designated reviewing official. The designated reviewing official shall then determine, within a reasonable period of time, whether or not to deny the access requested based on the standards stated in Section VII.B.5.b, "Reviewable Grounds for Denial" (see, Page 56), of these privacy policies.

The Privacy Officer shall then promptly provide written notice to the individual of the determination of the designated reviewing official and implement the designated reviewing official's determination.

7. Documentation.

The Privacy Officer shall maintain, or cause to be maintained, documentation of:

- a. The designated record sets that are subject to access by individuals; and,
- b. The titles of the persons or offices responsible for receiving and processing request for access by individuals.

The documentation shall be maintained by CSCSO in written or electronic form for six years after the date of its creation or the date when it was last in effect, whichever is later.

C. Right to Request Amendment.

1. Generally.

Except when access is denied under Section VII.C.5, “Grounds for Denying the Amendment” (see, Page 60) of these privacy policies, an individual shall have a right to have CSCSO amend protected health information or a record about the individual in a designated record set for as long as the protected health information is maintained in the designated record set.

2. Request for Amendment.

The individual’s request for amendment must be submitted in writing to the Privacy Officer and must state in the written request a reason to support the requested amendment. Individuals shall be informed in advance of these requirements in CSCSO’s Notice of Privacy Practices.

3. Action on Request for Amendment.

a. Time Limits for Action.

The Privacy Officer shall act on a request for access no later than sixty (60) calendar days after CSCSO’s receipt of the request.

If the Privacy Officer is unable to take an action on the request within that sixty (60) day period, the Privacy Officer may extend the time for the action by no more than thirty (30) calendar days, provided:

- (1) Within that sixty (60) day period, the Privacy Officer shall provide the individual with a written statement of the reason(s) for the delay and the date by which CSCSO will complete its action on the request; and,
- (2) Only one such extension shall be permitted on a request for amendment.

b. Inform Individual of Action on Request.

If the request for amendment is accepted, in whole or in part, the Privacy Officer shall inform the individual of the acceptance of the request and make the amendment requested in accordance with Section VII.C.3.a, above, of these privacy policies.

If the request for amendment is denied, in whole or in part, the Privacy Officer shall provide the individual with a written denial, in accordance with Section VII.C.6, “Actions if Amendment is Denied” (see, Page 61) of these privacy policies, and shall take the other actions required by that Section VII.C.6.

4. Accepting the Amendment.

If the individual’s request for amendment is accepted, in whole or in part, the Privacy Officer shall:

a. Making the Amendment.

The Privacy Officer shall make the appropriate amendment to the protected health information or record that is the subject of the request for amendment by, at a minimum, identifying the records in the designated record set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment.

b. Informing the Individual.

The Privacy Officer shall inform the individual as stated in Section VII.C.3.b, “Inform Individual of Action on Request” (see, Page 59) of these privacy policies, that the amendment has been accepted and obtain the individual’s identification of and agreement to have CSCSO notify the relevant persons that the amendment needs to be shared in accordance with Section VII.C.4.c, below.

c. Informing Others.

The Privacy Officer shall make a reasonable effort to inform and provide the amendment within a reasonable time to:

- (1) Persons identified by the individual as having received protected health information about the individual and needing amendment;
- (2) Persons, including CSCSO business associates, that CSCSO knows have the protected health information that is the subject of the amendment and that may have relied, or could

foreseeably rely, on such information to the detriment of the individual.

5. Grounds for Denying the Amendment.

An individual's request to amend protected health information may be denied if the Privacy Officer determines that the protected health information or record that is the subject of the request:

- a. Was not created by CSCSO, unless the individual provides a reasonable basis to believe that the originator of the protected health information is no longer available to act on the requested amendment;
- b. Is not part of the designated record set;
- c. Would not be available for inspection (see, Section VII.B.1, "Generally" on Page 53 of these privacy policies); or,
- d. Is accurate and complete.

6. Actions if Amendment is Denied.

If an individual's requested amendment is denied, in whole or in part, CSCSO shall comply with the following:

a. Written Denial.

The Privacy Officer shall provide a written denial to the individual within the applicable time period stated in Section VII.C.3.a, "Time Limits for Action" (see, Page 59) of these privacy policies. The denial shall contain:

- (1) The basis for the denial;
- (2) The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement;
- (3) A statement that, if the individual does not submit a statement of disagreement, the individual may request that CSCSO provide the individual's request for amendment and the denial with any future disclosures of the protected health information that is the subject of the requested amendment; and,

- (4) A description of how the individual may complain to CSCSO pursuant to CSCSO's complaint procedure or to the Secretary of the United States Department of Health and Human Services. The description shall include the name or title and telephone number of the contact person or office designed by CSCSO to receive complaints.

b. Statement of Disagreement.

The individual may submit a written statement disagreeing with the denial of all or part of a requested amendment and the basis for such disagreement.

c. Rebuttal Statement.

The Privacy Officer may prepare, or cause to be prepared, a written rebuttal of CSCSO to the individual's statement of disagreement. If a rebuttal statement is prepared, a copy of it shall be provided to the individual who submitted the statement of disagreement.

d. Recordkeeping.

As appropriate, the Privacy Officer shall identify the record or protected health information in the designated record set that is the subject of the disputed amendment and append or otherwise link the individual's request for amendment, CSCSO's denial of the request, the individual's statement of disagreement, if any, and CSCSO's rebuttal, if any, to the designated record set.

e. Future Disclosures.

- (1) If a statement of disagreement has been submitted by the individual, CSCSO will include the material appended in accordance with section VII.C.6.d, above, or, at the election of the Privacy Officer, an accurate summary of any such information, with any subsequent disclosure of the protected health information to which the disagreement relates.
- (2) If the individual has not submitted a written statement of disagreement, CSCSO will include the individual's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of the protected health information only if the individual has requested such action in accordance with Section

VII.C.6.a.(3), “Actions if Amendment is Denied” (see, Page 61) of these privacy policies.

- (3) When a subsequent disclosure described in (1) or (2), above, is made using a transaction that does not permit the additional material to be included with the disclosure, CSCSO shall separately transmit the material to the recipient of the transaction.

7. Documentation.

The Privacy Officer shall maintain documentation of the titles of the persons or offices responsible for receiving and processing requests for amendment. The documentation shall be maintained by CSCSO in written or electronic form for six (6) years after the date the notice was last in effect.

D. Right to an Accounting of Disclosures.

1. Right to Accounting.

a. General Rule.

Except as stated in VII.D.1.b, “Exceptions” or VII.D.1.c “Suspension of Right for Certain Disclosures”, below, an individual shall have a right to receive an accounting of disclosures of protected health information made by CSCSO in the six (6) years prior to the date on which the accounting is requested or for such shorter period as the individual may request.

b. Exceptions.

The right to an accounting of disclosures does not apply to the following types of disclosures:

- (1) To carry out treatment, payment and health care operations as provided in Section VI.D, “Uses and Disclosures to Carry Out Treatment, Payment and Health Care Operations” of these privacy policies (see, Page 16);
- (2) To individuals of protected health information about them;
- (3) Incident to a use or disclosure otherwise permitted or required by these privacy policies as provided in Section VI.B “Incidental Uses and Disclosures” (see Page 14);

- (4) Pursuant to an authorization as provided in Section VI.E “Uses and Disclosures for Which an Authorization is Required” of these privacy policies (see Page 17);
- (5) For the facility’s directory or to persons involved in the individual’s care or other notification purposes as provided in Section VI.F, “Uses and Disclosures Requiring an Opportunity for the Individual to Agree or Object” (see, Page 22) of these privacy policies);
- (6) For national security or intelligence purposes as provided in Section VI.G.11.c, “National Security and Intelligence Activities” (see, Page 40) of these privacy policies);
- (7) To correctional institutions or law enforcement officials as provided in Section VI.G.11.e, “Correctional Institutions and Other Law Enforcement Custodial Situations” (see, Page 41) of these privacy policies);
- (8) As part of a limited data set in accordance with Section VI.J “Limited Data Set” (see Page 47) of these privacy regulations; or,
- (9) That occurred prior to April 14, 2003.

c. Suspension of Right for Certain Disclosures.

An individual’s right to receive an accounting of disclosures to a health oversight agency (see, Section VI.G.5, “Uses and Disclosures for Health Oversight Activities” on Page 29 of these privacy policies) or to a law enforcement official (see, Section VI.G.7, “Disclosures for Law Enforcement Purposes” on Page 34 of these privacy policies) shall be temporarily suspended for the time specified by the agency or official, if the agency or official provides CSCSO 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.

If the agency or official statement is made orally, the Privacy Officer shall:

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

- (2) Temporarily suspend the individual's right to an accounting of disclosures subject to the statement; and,
- (3) Limit the temporary suspension to no longer than thirty (30) calendar days from the date of the oral statement, unless a written statement as described above is submitted during that time.

2. Content of the Accounting.

The written accounting provided to the individual shall meet the following requirements:

- a.** Except as otherwise stated in Section VII.D.1.b, "Exceptions" (see, Page 63) of these privacy policies, the accounting must include the disclosures of protected health information that occurred during the period the individual requests up to a maximum of six (6) years prior to the date of the request, including disclosures to or by business associates of CSCSO.
- b.** Except as stated in Section VII.D.2.c, "Multiple Disclosures for a Single Purpose" (see Page 65) or Section VII.D.2.d "Disclosures for Particular Research" (see Page 66) of these privacy policies, the accounting must include for each disclosure:
 - (1) The date of the disclosure;
 - (2) The name of the entity or person who received the protected health information and, if known, the address of such entity or person;
 - (3) A brief description of the protected health information disclosed; and,
 - (4) A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure; or, in lieu of such statement:
 - (a) A copy of a written request for disclosure by the Secretary of Health and Human Services under Section VI.G.14, "Disclosure to the Secretary of Health and Human Services" (see, Page 42) of these privacy policies, if any; or,

- (b) A copy of a written request for disclosure under Section VI.G, “Uses and Disclosures for which an Authorization or an Opportunity to Agree or Object is Not Required” (see, Page 24) of these privacy policies, if any.

c. Multiple Disclosures for a Single Purpose.

If, during the period covered by the accounting, CSCSO has made multiple disclosures of protected health information to the same person or entity for a single purpose under Section VI.G.14, “Disclosure to the Secretary of Health and Human Services” (see, Page 42) or Section VI.G, “Uses and Disclosures for which an Authorization or an Opportunity to Agree or Object is Not Required”(see, Page 24) of these privacy policies, the accounting may with respect to such multiple disclosures, provide:

- (1) The information required by Section VII.D.2.b (see, Page 75) of these privacy policies, for the first disclosure during the accounting period;
- (2) The frequency, periodicity, or number of the disclosures made during the accounting period; and,
- (3) The date of the last such disclosure during the accounting period.

3. Provision of the Accounting.

a. Time Limit to Provide the Accounting.

The Privacy Officer shall act on a request for an accounting no later than sixty (60) calendar days after CSCSO's receipt of the request.

Within that sixty (60) day period, the Privacy Officer shall:

- (1) Provide the individual with the accounting requested; or,
- (2) If the Privacy Officer is unable to take an action on the request within that sixty (60) day period, the Privacy Officer may extend the time for the action by no more than thirty (30) calendar days, provided:
 - (a) Within that sixty (60) day period, the Privacy Officer shall provide the individual with a written statement of the reason(s) for the delay and the date by which CSCSO will provide the accounting; and,
 - (b) Only one such extension shall be permitted on a request for amendment.

b. Fee for Accounting.

The first accounting to an individual in any twelve (12) month period will be provided to the individual without charge. For each subsequent request for an accounting by the same individual with the twelve (12) month period shall be as stated in Appendix F to these privacy policies; before charging the fee, however, the Privacy Officer shall notify the individual in advance of the fee and provide the individual an opportunity to withdraw or modify the

request for a subsequent accounting in order to avoid or reduce the fee. At any time and upon his/her discretion, the Privacy Officer may waive the fee.

c. Documentation.

The Privacy Officer shall document and retain the following:

- (1) The information required to be included in an accounting under Section VII.D.2, "Content of Accounting" (see, Page 65) of these privacy policies, for disclosures of protected health information that are subject to an accounting;
- (2) The written accounting that is provided to the individual under this section; and,
- (3) The titles of the persons of offices responsible for receiving and processing requests for an accounting by individuals.

The documentation shall be maintained by CSCSO in written or electronic form for six years after the date of its creation or the date when it was last in effect, whichever is later.

VIII. PERSONAL REPRESENTATIVES.

A. General Rule.

Except as otherwise stated or permitted in these privacy policies, CSCSO will treat a personal representative as the individual for purposes of these privacy policies.

B. Adults and Emancipated Minors.

If, under state law, a person has authority to act on behalf of an individual who is an adult or an emancipated minor in making decisions related to health care, CSCSO will treat such person as a personal representative with respect to protected health information relevant to such personal representative.

C. Unemancipated Minors.

1. General Rule.

If, under state law, a parent, guardian, or other person acting in loco

parentis has authority to act on behalf of an individual who is an unemancipated minor in making decisions related to health care, CSCSO will treat such person as a personal representative with respect to protected health information relevant to such personal representative.

Notwithstanding the general rule stated, above, a person will not be treated as a personal representative of an unemancipated minor, and the minor has the authority to act as an individual, with respect to protected health information pertaining to health care services, if:

- a. The minor consents to such health care service; no other consent to such health care services is required by state law, regardless of whether the consent of another person has also been obtained; and, the minor has not requested that such person be treated as the personal representative.
- b. The minor may lawfully obtain such health care service without the consent of a parent, guardian, or other person acting in loco parentis, and the minor, a court, or another person authorized by law consents to such health care service; or,
- c. A parent, guardian, or other person acting in loco parentis assents to an agreement of confidentiality between CSCSO and the minor with respect to such health care service.

2. Exception.

Notwithstanding the preceding subparagraph 1:

- a. If, and to the extent, permitted or required by an applicable provision of state or other law, including applicable case law, a covered entity may disclose, or provide access in accordance with Section VII.B “Right of Access” (see Page 53) of these privacy policies to protected health information about an unemancipated minor to a parent, guardian, or other person acting *in loco parentis*;
- b. If, and to the extent, prohibited by an applicable provision of state or other law, including applicable case law, CSCSO may not disclose, or provide access in accordance with Section VII.B “Right of Access” (see Page 53) of these privacy policies to, protected health information about an unemancipated minor to a parent, guardian, or other person acting *in loco parentis*; and,
- c. Where the parent, guardian, or other person acting *in loco parentis*, is not the personal representative under subparagraphs VIII.C.1.a,

VIII.C.1.b and VIII.C.1.c of this Section VIII.C “Unemancipated Minors” (see Page 68) of these privacy policies and where there is no applicable access provision under state or other law, including case law, CSCSO may provide or deny access under Section VII.B “Right of Access” (see Page 53) of these privacy policies to a parent, guardian, or other person acting *in loco parentis*, if such action is consistent with state or other applicable law, provided that

such decision must be made by a licensed health care professional, in the exercise of professional judgment.

D. Deceased Individuals.

If under state law an executor, administrator, or other person has authority to act on behalf of a deceased individual or of the individual’s estate, CSCSO will treat that person as a personal representative under these privacy policies with respect to protected health information relevant to such person representation.

E. Abuse, Neglect, Endangerment Situations.

Notwithstanding anything in state law or these privacy policies to the contrary, CSCSO may elect not to treat a person as the personal representative of an individual if:

1. CSCSO has a reasonable belief that:
 - a. The individual has been or may be subjected to domestic violence, abuse, or neglect by such person; or,
 - b. Treating that person as the personal representative could endanger the individual; and
2. CSCSO, in the exercise of professional judgment, decides that it is not in the best interest of the individual to treat the person as the individual’s personal representative.

IX. DEFINITIONS.

A. Authorized Member of CSCSO’s Workforce.

“Authorized member of CSCSO’s workforce” means a member of CSCSO’s workforce who has been authorized to take the action involved by: (a) his or her job description; (b) a protocol established by the Privacy Officer; or, (c) by the Privacy Officer.

B. Business Associate.

“Business associate” means, with respect to CSCSO, a person or other legal entity that:

1. On behalf of CSCSO, but other than as a member of CSCSO’s workforce, performs, or assists in the performance of:
 - a. A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or,
 - b. Any other function or activity regulated by the HIPAA privacy rule; or
2. Provides, other than as a member of CSCSO’s workforce, legal, actuarial, accounting consulting, data aggregation, management, administrative, accreditation, or financial services to or for CSCSO, where the provision of such service involves the disclosure of individually identifiable health information from CSCSO, or from another business associate of CSCSO, to the person or legal entity.

C. Covered Entity.

“Covered entity” means a health plan, a health care clearinghouse, or a health care provider that is covered by the HIPAA privacy rule.

D. Designated Record Set.

“Designated record set” means a group of records maintained by or for CSCSO that is:

1. The medical records and billing records about individuals maintained by or for CSCSO; or,
2. Used, in whole or in part, by or for CSCSO to make decisions about individuals.

For purposes of this definition, the term “record” means any item, collection, or grouping of information that includes protected health information and is

maintained, collected, used, or disseminated by or for CSCSO.

E. Disclosure.

“Disclosure” means the release, transfer, provision of access to, or divulging in any other manner of information outside CSCSO.

F. Health Care Operations.

“Health care operations” means any of the following activities of CSCSO to the extent that the activities are related to covered functions:

1. Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such 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 individuals with information about treatment alternatives; and related functions that do not include treatment;
2. Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;
3. Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
4. Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and,
5. Business management and general administrative activities of CSCSO, including, but not limited to:
 - a. Management activities relating to implementation of and compliance with the requirements of these privacy policies and the HIPAA privacy rule;
 - b. Customer service;

- c. Resolution of internal grievances;
- d. The sale, transfer, merger, or consolidation of all or part of CSCSO with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and,
- e. Consistent with the applicable requirements of Section II.B, “De-Identification of Health Information” (see, Page 2), creating de-identified health information or a limited data set, and fundraising for the benefit of CSCSO, and marketing for which an individual authorization is not required.

G. Health Care.

“Health care” means care, services, or supplies related to the health of an individual.

“Health care” includes, but is not limited to, the following:

1. Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and,
2. Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

H. Health Oversight Agency.

“Health oversight agency” means an agency or authority of the United States, a state, a territory, a political subdivision of a state or territory, or an Indian tribe that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

“Health oversight agency” includes the employees or agents of such a public agency or its contractors or persons or entities to whom it has granted authority.

I. HIPAA Privacy Rule.

“HIPAA privacy rule” means 45 CFR Part 160 and 45 CFR Part 164 as amended from time to time.

J. Inmate.

“Inmate” means a person incarcerated in or otherwise confined to a correctional institution.

K. Law Enforcement Official.

“Law enforcement official” means an officer or employee of any agency or authority of the United States, a state, a territory, or an Indian tribe, who is empowered by law to:

1. Investigate or conduct an official inquiry into a potential violation of law; or,
2. Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

L. Payment.

“Payment” means the activities undertaken by CSCSO to obtain reimbursement for the provision of health care that relate to the individual for whom health care is provided.

“Payment” includes but is not limited to:

1. Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts) and adjudication or subrogation of health benefit claims;
2. 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;
3. Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;
4. Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and,
5. Disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement:
 - a. Name and address;

- b. Date of birth;
- c. Social security number;
- d. Payment history;
- e. Account number;
- f. Name and address of CSCSO.

M. Personal Representative.

“Personal representative” means a person who, under applicable law, has authority to act on behalf of an individual in making decisions related to health care.

N. Secretary of Health and Human Services.

“Secretary of Health and Human Services” means the Secretary of the United States Department of Health and Human Services or any other officer or employee of that Department to whom the authority involved has been delegated.

O. These Privacy Policies.

“These privacy policies” means these privacy policies adopted by CSCSO concerning the protection of the privacy of protected health information.

P. Treatment.

“Treatment” means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to an individual; or the referral of an individual (individual) for health care from one health care provider to another.

Q. Use.

“Use” means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of that information within CSCSO.

R. Workforce.

“Workforce” means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for CSCSO, is under the direct control of

CSCSO, whether or not they are paid by CSCSO.

APPENDIX A

Identification of Workforce Members' Access To Protected Health Information.

- (1) Executive Program Director: Executive Program Director must have access to all protected health information maintained by the private provider agency. There are no conditions applicable to that access.
- (2) Office Manager: The Office Manager must have access to any and all financial information concerning individuals served or supported by CSCSO. There are no conditions applicable to that access.
- (3) Human Resource Manager: Human Resource Manager must have access to all protected health information maintained by the private provider agency. There are no conditions applicable to that access.
- (4) Direct Support Professional: Direct Support Staff must have access to all health/clinical information of individuals whom she/he supports. There are no conditions applicable to that access. She/he must have access to billing information concerning an individual if the Accounting Staff must discuss billing matters concerning that individual with the Direct Support Staff.
- (5) Home Supervisor: Home Supervisors must have access to all health/clinical information of individuals whom she/he supports. There are no conditions applicable to that access. She/he must have access to billing information concerning an individual if the Accounting Staff must discuss billing matters concerning that individual with the Home Supervisors.
- (6) Program Coordinator: Program Coordinators must have access to all health/clinical information of individuals whom she/he supports. There are no conditions applicable to that access. She/he must have access to billing

information concerning an individual if the Accounting Staff must discuss billing matters concerning that individual with the Program Coordinators.

- (7) Senior Program Coordinator: Senior Program Coordinators must have access to all health/clinical information of individuals whom she/he supports. There are no conditions applicable to that access. She/he must have access to billing information concerning an individual if the Accounting Staff must discuss billing matters concerning that individual with the Senior Program Coordinators.
- (8) Accounting Staff: The Accounting Staff must have access to all billing and payment information concerning the individual. There are no conditions applicable to that access. She/he must have access to health/clinical information concerning the individual to the extent necessary to bill for services provided to the individual.
- (9) Receptionist: The Receptionist must have access to the names of all individuals and of their personal representatives. The Receptionist must have access to individual information related to receiving faxes, filing and medical supply orders. There are no conditions applicable to that access.
- (10) Janitorial/Maintenance Staff: The Janitorial/Maintenance Staff does not need access to any protected health information concerning any individual of CSCSO.

APPENDIX B

Fees for Copies of Protected Health Information

- postage (if applicable)
- copy fee = ten cents (\$.10) per page
- At any time and upon his/her discretion, the Privacy Officer may waive the fee.

APPENDIX C

Fees for Accounting

- For the first accounting in a twelve (12) month period - No Charge.
- For the second or greater accounting in a twelve (12) month period – ten cents (\$.10) per page plus postage (if applicable).
- At any time and upon his/her discretion, the Privacy Officer may waive the fee.

CENTRAL STATE COMMUNITY SERVICES OKLAHOMA
POLICIES FOR PROTECTION OF THE PRIVACY
OF
PROTECTED HEALTH INFORMATION

INDEX

Abuse	22, 33, 34, 36, 37, 42, 43, 46, 84, 87
Accounting of Disclosures	76, 77, 78
Content of Accounting	82
Fee for Accounting	81
Provision of the Accounting	81
Right to Accounting	76
Suspension of Right	76, 78
Actions if Access is Denied	
Denial of Access	66, 68, 69
Administrative Policies	5
Affiliated Covered Entity	5
Amended Protected Health Information	9
Receipt of	9, 17, 18, 24, 38, 66, 72, 81
Amendment of Information	
Accepting the Amendment	73
Actions if Amendment is Denied	73, 74, 76
Grounds for Denying the Amendment	72, 74
Request for Amendment	72, 73, 75, 76, 81
Amendment Request	
Accepting the Amendment	73
Action on Request for Amendment	72
Actions if Amendment is Denied	73, 74, 76
Request for Amendment	72, 73, 75, 76, 81
Authorization or Opportunity to Agree	64
Authorization Required	48
Compound Authorization	24, 27
Conditioning of Authorization	24, 26
Form of Authorization	23, 25
Maintaining an Authorization	24
Prior Authorizations	22, 62
What is a Valid Authorization	23
Business Associate	85
Business Associates	14, 55, 74, 78
Cadaveric Organ, Eye or Tissue Donation	47

Changes.....	8, 11, 12, 13
Changes in Law.....	11
Practices Not Stated In Notice of Privacy Practices.....	13
Practices Stated In Notice of Privacy Practices.....	11
Complaints.....	6, 7, 9, 71, 75
Complaint against CSCSO.....	9
Contact Person.....	6, 7, 71, 75
Coroners.....	23, 46
Correctional Institutions.....	52, 77
Data Use Agreement.....	58, 59
Decedents.....	23, 45, 46, 48
Definitions.....	84
Authorized member of CSCSO's workforce.....	84
Business associate.....	85
Covered entity.....	86
Designated record set.....	86
Disclosure.....	86
Health care.....	88
Health care operations.....	86
Health oversight agency.....	88
HIPAA privacy rule.....	88
Inmate.....	88
Law enforcement official.....	89
Payment.....	89
Psychotherapy notes.....	90
Secretary of Health and Human Services.....	90
These privacy policies.....	90
Treatment.....	90
Use.....	91
Workforce.....	91
De-Identification.....	2, 87
Removal of Identifiers.....	3
Designated Record Set.....	67, 71, 73, 74, 75, 86
Designee.....	15
Disaster Relief.....	32
Disclaimer.....	1
Discovery Request.....	39, 40
Documentation....	3, 6, 7, 8, 9, 10, 12, 13, 17, 18, 20, 21, 28, 40, 41, 48, 60, 61, 71, 72, 76, 81, 82
Retention.....	12, 13
Domestic Violence.....	33, 36, 43, 46, 84
Emancipated Minors.....	82
Facility Directories.....	28, 64
Funeral Directors.....	46
Health Oversight Activities.....	23, 37, 78
Health Oversight Agency.....	38, 54, 78, 88

Hybrid Entity	5
Incidental Uses and Disclosures	18, 77
Inmate	16, 52, 69, 88
Intelligence Activities	51, 77
Intimidating or Retaliatory Acts	9, 10
judicial and administrative proceedings.....	42
Judicial and Administrative Proceedings.....	33, 39
Law Enforcement.....	33, 37, 42, 43, 44, 45, 46, 49, 52, 54, 60, 77, 78, 89
Law Enforcement Custodial Situations	77
Law Enforcement Official	43, 45, 52, 89
Limited Data Set	58, 59, 77, 87
Marketing.....	35, 56, 57, 87
Disclosures for Marketing.....	56
Medical Examiners	23, 46
Military	51
Armed Forces.....	51
Foreign Military	51
Veterans	51
Minimum Necessary	18, 19, 20
Mitigation.....	10
Multiple Covered Functions	6
National Security	51, 77
Neglect.....	33, 34, 36, 37, 42, 43, 46, 84
Notice of Privacy Practices.....	6, 7, 11, 12, 13, 16, 17, 18, 26, 72
Form of Notice.....	16
Posting	17, 36
Provision of Notice	12, 16
Order	39, 40, 43, 51, 52, 61
Organized Health Care Arrangement.....	6, 85, 86
Personal Representatives	60, 82, 93
Abuse, Neglect, Endangerment Situations.....	84
Adults.....	82
Emancipated Minors	82
Unemancipated Minors.....	82, 83
Persons Involved in the Individual's Care	
When the Individual Is Not Present.....	31, 32
When the Individual Is Present.....	30, 32
Privacy Officer.....	2, 3, 5, 6, 8, 9, 10, 11, 12, 13, 14, 15, 16, 18, 19, 20, 21, 24, 33, 34, 36, 37, 38, 39, 42, 46, 47, 49, 50, 52, 53, 54, 55, 56, 57, 58, 71, 75, 76, 81, 84, 94
Privacy Protection.....	62, 63
Restriction of Uses and Disclosures	63
Restriction on Means and Location of Communications.....	65
Psychotherapy Notes.....	13, 14, 22, 27
Public Health Activities	33, 34
Public Officials	20, 61

Qualified Protective Order	40, 41
Questions.....	14, 60
Re-Identification	5
Required by Law.....	14, 18, 19, 23, 33, 36, 42, 43, 44, 59
Research.....	20, 21, 24, 25, 27, 47, 48, 49, 58, 62, 63, 69, 78, 80
Revision of Notice	11, 18
Revocation of an Authorization	28
Right of Access.....	7, 64, 66, 68, 69, 83, 84
Action on Request for Access.....	66, 68
Actions if Access is Denied.....	67, 70
Providing Access	67, 68
Request for Access.....	66, 67, 68, 70, 71, 72
Safeguards.....	8, 18, 59, 94
Sanctions.....	9, 10
Satisfactory Assurance.....	14, 39, 40, 41
Secretary of Health and Human Services	11, 19, 23, 53, 79, 90
Specialized Government Functions	50
State Law	1, 82, 83, 84
Statistical and Scientific.....	3
Subpoena.....	39, 40, 43, 61
Threat to Health or Safety.....	49, 62
Training.....	8, 21, 22, 87
Verification of Identity and Authority	60
Veterans	51
Victims of a Crime.....	9, 44, 54
Victims of Abuse, Neglect or Domestic Violence.....	36
Violations, Reporting	
Reporting.....	14, 34, 42, 43, 45, 54, 89
Waiver of Rights.....	11
Web Site.....	17
Whistleblowers	9, 54
Workers' Compensation	52, 53
Workforce	1, 2, 7, 8, 9, 10, 11, 14, 15, 19, 20, 24, 28, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 42, 43, 44, 45, 46, 47, 49, 50, 51, 52, 53, 54, 55, 56, 57, 60, 62, 64, 84, 85, 91, 92