Cottonwood, Incorporated
Policies and Procedures

SECTION: Consumer Related **POLICY NO:** 05-048

SUBJECT: Privacy of Protected Health Information **PAGE(S):** 1 of 93

EFFECTIVE DATE: November 2008

COTTONWOOD, INC.

POLICIES FOR PROTECTION OF THE PRIVACY AND SECURITY OF PROTECTED HEALTH INFORMATION

TABLE OF CONTENTS

M. Health Oversight Agency
N. HIPAA Breach Notification Rule
O. HIPAA Privacy Rule
P. HIPAA Security Rule
Q. Information System
R. Inmate
S. Integrity
T. Law Enforcement Official
U. Malicious Software
V. Password
W. Payment
X. Physical Safeguards
Y. Privacy Officer
AA. Secretary of Health and Human Services
BB. Security Officer
CC. Security or Security Measures
DD. Security Incident
EE. Technical Safeguards
FF. These Privacy and Security Policies
GG. Treatment
HH. Unsecured Protected Health Information
II. Use
JJ. Workforce

APPENDIX A

COTTONWOOD, INC.

POLICIES FOR PROTECTION OF THE PRIVACY AND SECURITY OF PROTECTED HEALTH INFORMATION

I.INTRODUCTION

A.Purpose of These Privacy and Security Policies

These Privacy and Security Policies 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, breach notification, and privacy regulations at 45 CFR Part 160 and Part 164.

These policies are designed to reasonably ensure the confidentiality, integrity, and availability of all electronic protected health information that Cottonwood, Inc., creates, receives, maintains, or transmits; protect against any reasonably anticipated threats or hazards to the security or integrity of such information; protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the HIPAA Privacy Rule and Cottonwood, Inc.'s Privacy and Security Policies; and to ensure compliance with the HIPAA Security regulation by Cottonwood, Inc.'s workforce.

In all instances, these Privacy and Security 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 and Security 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 and procedures contained or referred to in these Privacy and Security Policies, or that may be added or otherwise established by Cottonwood, Inc. in the future, represent the policies established by Cottonwood, Inc. for the members of its workforce in relation to the particular subject addressed by the policy. It is the intention of Cottonwood, Inc. that these Privacy and Security Policies be used by its employees, and other members of its workforce, in meeting their responsibilities to Cottonwood, Inc. Violation of a policy can be the basis for discipline or termination of employment; however, because these Privacy and Security Policies relate to the establishment and maintenance of high standards of

performance, under no circumstances shall any policy or procedure 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 Cottonwood, Inc., 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 Cottonwood, Inc. that is individually identifiable except: (a) employment records held by Cottonwood, Inc. in its role as an employer; and, (b) information regarding a person who has been deceased for more than fifty (50) years.

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

1.Is created or received by a 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 Cottonwood, Inc. 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 Cottonwood, Inc.'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 are 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 IV.N and Section IV.O of these Privacy and Security 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 Cottonwood, Inc. 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 publicly 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 is 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 of these Privacy and Security 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 Cottonwood, Inc. 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.ELECTRONIC PROTECTED HEALTH INFORMATION

"Electronic Protected Health Information" is any protected health information maintained by Cottonwood, Inc. that is transmitted by electronic media or maintained in electronic media.

"Electronic Media" means:

"(1)Electronic storage material on which data is or may be recorded electronically, including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card;

(2)Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, Extranet or Intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission."

IV.ADMINISTRATIVE POLICIES

A.Designation of Privacy Official and Security Official

1.Designation of Privacy Official

Cottonwood, Inc.'s Chief Executive Officer shall designate a privacy official who shall be responsible for the development, updating and implementation of Cottonwood, Inc.'s privacy policies. That privacy official shall be called the "Privacy Officer" of Cottonwood, Inc. The privacy

official may be the same individual who is designated as the security official of Cottonwood, Inc.

Cottonwood's Privacy Officer will be the Administrator of Services. The record of such designation will be maintained as incorporated in this policy.

2.Designation of Security Official

Cottonwood, Inc.'s Chief Executive Officer shall designate a security official who shall be responsible for the development, updating and implementation of Cottonwood, Inc.'s security policies. That security official shall be called the "Security Officer" of Cottonwood, Inc.

Cottonwood's Security Officer will be the Computer Network Manager. The record of such designation will be maintained as incorporated in this policy.

3.Documentation

Cottonwood, Inc.'s Chief Executive Officer shall maintain, or cause to be maintained, a written or electronic record of the designation of the Privacy Officer and of the Security 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

Cottonwood, Inc.'s Chief Executive Officer shall designate a contact person or office who shall:

a. Be responsible for receiving complaints concerning Cottonwood, Inc.'s privacy and breach notification policies and procedures, Cottonwood, Inc.'s compliance with those policies and procedures, or Cottonwood, Inc.'s compliance with the HIPAA Privacy and Breach Notification Rules pursuant to relevant sections of these Privacy and Security Policies; and,

b. Provide further information about matters covered by Cottonwood, Inc.'s Notice of Privacy Practices.

c. The Director of Support Services and/or the Director of CDDO Administration are designated by the CEO to hear complaints and provide further information about Cottonwood's privacy practice.

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

The CEO designates the following positions as responsible for receiving and processing access to amendments to protected Health Information"

a. Case Manager
b. Director of Support Services
c. Director of CDDO Administration

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

Cottonwood, Inc.'s Chief Executive Officer 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 VIII.C "Right to Request Amendment" of these policies.

The CEO designates the following positions as responsible for amending health care information.

a. Case Manager
b. Nurse
c. Director of CDDO Administration

4.Documentation.

The record of such designations will be maintained as incorporated in this policy.

C.Identification of Workforce Members' Access To Protected Health Information

Attached to these policies as Appendix A is an identification of those classes of Cottonwood, Inc.'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.
The Policy Committee will review the identification and categories stated in Appendix A and made such changes to Appendix A as the Committee determines is necessary or desirable to keep Appendix A current.

D.Training of Workforce

All staff members of Cottonwood shall be trained in HIPAA guidelines when these privacy policies come into effect. Thereafter, each new member of the workforce shall be trained within sixty (60) 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 thirty (30) 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 Cottonwood'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 Cottonwood'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 either the Case Manager, Nurse or Director of CDDO Administration.

G.Process for Individuals to Make Complaints

Individuals who desire to make a complaint against Cottonwood concerning Cottonwood's privacy policies and procedures, its compliance with those policies and procedures, or the requirements of the HIPAA privacy rule shall submit the complaint to Support Services Director or the Director of CDDO Administration in writing.

The individuals above shall implement the Cottonwood grievance procedure.

Written documentation of each complaint and its disposition will be maintained 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.Disciplinary Sanctions

Each member of Cottonwood's workforce must report any actual or possible violation of Cottonwood'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. Any violations of the HIPAA privacy rule could result in disciplinary action up to and including termination.

Examples of violations are:

a. Failure to promptly report any violation of any Cottonwood privacy policy or procedure or requirement of the HIPAA privacy rule to the Privacy

Officer.

b. Inadvertent violation of any Cottonwood privacy policy or requirement of the HIPAA privacy rule.
c. Knowing violation of any Cottonwood privacy policy or requirement of the HIPAA privacy rule.
d. Knowingly and improperly obtaining or disclosing protected health information.
e. Obtaining protected health information under false pretenses.
f. Obtaining or disclosing protected health information with the intent to sell, transfer or use it for commercial advantage, personal gain or malicious harm.

The Human Resources Director shall maintain written documentation or disciplinary action, if any, in written or electronic form for six (6) years after the date of 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 Cottonwood, Inc.'s workforce or an Cottonwood, Inc. business associate in violation of Cottonwood, Inc.'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 Cottonwood, Inc.

J.Prohibition on Intimidating or Retaliatory Acts

Neither Cottonwood, Inc. nor any member of Cottonwood, Inc.'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, breach notification and security policies or the HIPAA regulations, including filing a complaint under the HIPAA Privacy Rule or under these 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 Administrative Simplification provisions of HIPAA;

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 regulations, 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 Cottonwood, Inc.'s workforce may require an individual to waive the individual's rights under these privacy and breach notification policies or the HIPAA Privacy or Breach Notification Rules, or his or her right to file a complaint with the Secretary of HHA, 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.

As a function of the Policy Committee, the Privacy Officer shall promptly change these privacy and breach notification policies as necessary and appropriate to comply with changes in the law, including changes in the HIPAA Privacy and Breach Notification Rules. The changed policy or procedure shall be promptly documented and implemented. If the change materially affects the content of Cottonwood, Inc.'s Notice of Privacy Practices, the Privacy Officer shall promptly make the appropriate revisions to the notice in accordance with Section VI.D "Revision of Notice of Privacy Practices" of these Privacy and Security Policies.

The Security Officer shall promptly change these security policies and procedures as necessary and appropriate to comply with changes in the law, including changes in the HIPAA Security Rule, and to respond to environmental or operational changes. The changed policy or procedure shall be promptly documented and implemented.

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

When Cottonwood, Inc. changes a privacy practice that is stated in its Notice of Privacy Practices and makes corresponding changes to Cottonwood, Inc.'s policies, the change shall be effective for protected health information Cottonwood, Inc. 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 and Breach Notification Rules;

b.The Privacy Officer documents the policy or procedure, as revised, as stated in "Documentation" and "Period of Retention" of these Privacy and Security 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 "Provision of Notice of Privacy Practices" of these Privacy and Security 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

Cottonwood, Inc. 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 and Breach Notification Rules and the change is per policy & procedure guidelines.

N.Documentation

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

a.Maintain these Privacy and Security Policies and procedures in written or electronic form;

b.If a communication is required by these Privacy and Security Policies and procedures, or by the HIPAA regulations, 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 and Security Policies and Procedures, or by the HIPAA regulations, to be documented, maintain a written or electronic record of that action, activity or designation.

O.Period of Retention

Documentation required by "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.

P.Business Associates

Prior to Cottonwood, Inc. 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 Cottonwood, Inc.'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 HIPAA Privacy and Security Rules.

However, if the business associate is required by law to perform a function or activity on behalf of Cottonwood, Inc. or to provide a service described in the HIPAA Privacy Rule's definition of a business associate (see, Section XII.G, "Business Associate") to Cottonwood, Inc., Cottonwood, Inc. 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. Cottonwood, Inc. 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 Cottonwood, Inc. 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 and Security Policies and the HIPAA Privacy Rule prior to being signed on behalf of Cottonwood, Inc.

Q.Reporting Violations

Each member of Cottonwood, Inc.'s workforce must report any actual or possible violation of these Privacy and Security Policies or the HIPAA Privacy, Breach Notification, or Security Rule to the Privacy Officer or the Security Officer as soon as he or she becomes aware of the actual or possible violation.

R.Questions Concerning HIPAA Compliance

If any member of Cottonwood, Inc.'s workforce has a question concerning Cottonwood, Inc.'s privacy or breach notification policies, the HIPAA Privacy or Breach Notification Rules, or their application to any situation, he or she should contact the Privacy Officer for guidance. If any member of Cottonwood, Inc.'s workforce has a question concerning Cottonwood, Inc.'s security policies, the HIPAA Security Rule, or its application to any situation, he or she should contact the Security Officer for guidance. Either the Privacy Officer or the Security Officer may contact legal counsel for legal advice as he or she believes is necessary or desirable.

S.Action by Designee

Whenever an action may be or is required to be taken under these Privacy and Security Policies by the Privacy Officer, Security Officer, The Director of Support Services, or any other member of Cottonwood, Inc.'s workforce, the action may be taken by that person's designee.

V.COTTONWOOD, INC. 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 Cottonwood, Inc.'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 Cottonwood, Inc.'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 Director of Support Services, Nurse, and Director of CDDO Administration 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 Cottonwood, Inc.'s workforce desires to request protected health information from another provider, a health plan or a health care clearinghouse and the request is not routine, he or she shall review that request with his/her supervisory who will use the following criteria:

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.

VI.NOTICE OF PRIVACY PRACTICES

A.Form of Notice of Privacy Practices.

The Notice of Privacy Practices used by Cottonwood, Inc. shall be reviewed from time to time by the Policy Committee and Privacy Officer to ensure that it meets 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, Cottonwood, Inc.'s Notice of Privacy Practices shall be provided to any individual who receives services or supports from Cottonwood, Inc. (except to an inmate of a correctional institution) no later than the date of the first service delivery by Cottonwood, Inc. and to other persons upon request. In an emergency treatment situation, Cottonwood, Inc.'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 Cottonwood, Inc.'s office 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. The transmission of the Notice of Privacy Practices by e-mail will be accomplished by Case Manager or CDDO Liaison. 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; his or her request should be submitted to Case Manager or CDDO Liaison.

2.Posting

Cottonwood, Inc.'s Notice of Privacy Practices shall be prominently posted on the Building I hallway bulletin board.

3.Web Site

Cottonwood, Inc.'s Notice of Privacy Practices shall be prominently posted on Cottonwood, Inc.'s web site and made available electronically through

the web site.

C.Obtaining Acknowledgment of Receipt of Notice of Privacy Practices

The Cottonwood staff member who provides Cottonwood's Notice of Privacy Practices to an individual in conjunction with the date of first service delivery shall obtain a written acknowledgement of the individual's receipt of the Notice of Privacy Practices. The written acknowledgement shall be the signature page of the back of the notice and will be filed in consumer case records.

If the individual's written acknowledgement cannot be obtained, the staff member(s) who attempted to obtain it shall document their good faith efforts to obtain the acknowledgement and the reason why it was not obtained. That documentation shall be on the same signature page and filed in case records.

D.Revision of Notice of Privacy Practices

Whenever there is a material change to the uses or disclosures, the individual's rights, Cottonwood, Inc.'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 Cottonwood, Inc. and of each written acknowledgment of receipt of the notice or documentation of good faith efforts to obtain such acknowledgment shall be maintained by Cottonwood, Inc. in written or electronic form for six (6) years after the date the notice was last in effect.

VII.USES AND DISCLOSURE OF PROTECTED HEALTH INFORMATION

A.General Rule

Except as otherwise stated in this section, Cottonwood, Inc. shall obtain the individual's written authorization in accordance with these Privacy and Security 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 and Security Policies or the HIPAA Privacy

Rule is permissible provided: (1) the applicable requirements of "Use and Disclosure of Only the Minimum Necessary Information," below, are met; 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, "Safeguards to Protect the Privacy of Protected Health Information").

C.Use and Disclosure of Only the Minimum Necessary Information

1.General Rule

Except as stated below, when using or disclosing protected health information, to the extent practical, members of Cottonwood, Inc.'s workforce shall limit protected health information to the limited data set, or if needed, to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

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 and Security Policies.

d.Disclosures made to the Secretary of Health and Human Services in accordance with the HIPAA regulations.

e.Uses or disclosures that are required by law.

f. Uses or disclosures that are required for Cottonwood, Inc.'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 Department Directors shall from time to time develop and implement policies and procedures that limit the protected health information requested 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 Privacy Officer 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 Cottonwood, Inc.'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 "Uses and Disclosures for which an Authorization or an Opportunity to Agree or Object is Not Required" of these Privacy and Security 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 Cottonwood, Inc.'s workforce or a business associate of Cottonwood, Inc. for the purpose of providing professional services to Cottonwood, Inc., if the professional represents that the information requested is the minimum necessary for the stated purpose(s); or,

d.Documentation or representations that comply with the applicable requirements of "Uses and Disclosures for Research Purposes" of these Privacy and Security Policies have been provided by the person requesting the information for research purposes.

The basis for reliance under this section shall be documented by the Case Manager, Nurse or CDDO staff person. That documentation shall be maintained in the individual's case record.

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

Cottonwood, Inc. 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 Cottonwood, Inc. 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; patient safety activities (as defined in 42 CFR 3.20); population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; 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 and Security Policies, Cottonwood, Inc. will not use or disclose protected heath information without an authorization that is valid under this Section VII. When Cottonwood, Inc. obtains or receives a valid authorization for its use or disclosure of protected health information, Cottonwood, Inc.'s use or disclosure must be consistent with that authorization.

2.Sale of Protected Health Information

Notwithstanding any provision of these Privacy and Security Policies, Cottonwood, Inc. will obtain an authorization for any disclosure of protected health information for which the disclosure is in exchange for direct or indirect remuneration from or on behalf of the recipient of the protected health information. Such authorization shall state that the disclosure will result in remuneration to Cottonwood, Inc.

This does not apply, however, to disclosures of protected health information:

a.For public health purposes as stated in applicable sections in these privacy and Security Policies;

b.For research purposes as stated in applicable sections of these Privacy and Security Policies, where the only remuneration received by Cottonwood, Inc. is a reasonable cost-based fee to cover the cost to prepare and transmit the protected health information for such purposes;

c.For treatment and payment purposes as stated in applicable sections of these Privacy and Security Policies;

d.For the sale, transfer, merger, or consolidation of all or part of Cottonwood, Inc. and for related due diligence as described in applicable sections of the definition of health care operations of these Privacy and Security Policies;

e.To or by a business associate for activities that the business associate undertakes on behalf of Cottonwood, Inc. pursuant to applicable sections of these Privacy and Security Policies, and the only remuneration provided is by Cottonwood, Inc. to the business associate for the performance of such activities;

f.To an individual, when requested under applicable sections of these Privacy and Security Policies;

g.Required by law as permitted by applicable sections of these Privacy and Security Policies; and,

h.Permitted by and in accordance with the applicable requirements of the HIPAA Privacy Rule, where the only remuneration received by Cottonwood, Inc. is a reasonable, cost-based fee to cover the cost to prepare and transmit the protected health information for such purpose or a fee otherwise expressly permitted by law.

3.What is a Valid Authorization?

An authorization is valid if it contains all the elements required by "Form of Authorization" of these Privacy and Security 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 Cottonwood, Inc. 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 Cottonwood, Inc. to have been revoked;

d. The authorization lacks a required element of these Privacy and Security Policies;

e.The authorization violates the requirements concerning compound authorizations of these Privacy and Security Policies;

f.The authorization violates the requirements concerning conditioning of these Privacy and Security Policies; or,

g. If any material information in the authorization is known by Cottonwood, Inc. to be false.

If any member of Cottonwood, Inc.'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 Director of Support Services or the Director of CDDO Administration.

4.Maintaining an Authorization

All authorizations shall be filed by the staff who received or generated the authorization.

5.Conditioning of Authorizations

e.General Rule

Except as stated in "Exceptions," below, Cottonwood, Inc. will not condition treatment or payment to an individual on the receipt of an authorization from that individual.

f.Exceptions

Cottonwood, Inc. may condition treatment or payment to an individual on the receipt of an authorization from that individual in the following situations:

(1)**Research.** Cottonwood, Inc. 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.** Cottonwood, Inc.. 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.

6.Form of Authorization

g.Required Elements - Generally

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 Cottonwood, Inc. 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.

h.Required Elements - Specific

The Privacy Rule requires certain things to be in the authorization if the authorization is for certain purposes.

(1)**Marketing.** If a disclosure for marketing involves direct or indirect financial remuneration to Cottonwood, Inc. from a third party, the authorization must state that such remuneration is involved. See, Section VII.H of these Privacy and Security Policies.

(2)**Sale of Protected Health Information**. If the disclosure is in exchange for direct or indirect remuneration from or on behalf of the recipient of the protected health information, the authorization must state that the disclosure will result in remuneration to Cottonwood, Inc.

i.Additional Elements

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

j.Plain Language

An authorization must be written in plain language.

k.Copy to Individual

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

7.Compound Authorizations

Cottonwood will not use compound authorizations.

8.Revocation of an Authorization

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

A written revocation should be submitted to the staff initiating the authorization who will cause the revocation to be filed in the case record.

9.Documentation

The staff initiating the authorization 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 Cottonwood, Inc.'s workforce may use or disclose protected health information without the individual's written authorization for the purposes described in this section 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. The individual's agreement or objection may be oral or written.

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

a.General Rules

(1)**Those Involved in Care**. Members of Cottonwood, Inc.'s workforce may, in accordance with 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 health care or payment related to that individual's health care.

(2)**Notification of Location, Condition, or Death**. Members of Cottonwood, Inc.'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 sections 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 Cottonwood, Inc.'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, 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 Cottonwood, Inc.'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 or needed for notification purposes.

(2) Other Actions. A member of Cottonwood, Inc.'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.

d.Disaster Relief

A member of Cottonwood, Inc.'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 "Notification of Location, Condition, or Death". However, the requirements of "When the Individual Is Present", "When the Individual Is Not Present", and "When the Individual is Deceased" of these Privacy and Security Policies apply to those uses and disclosures to the extent that the Cottonwood, Inc. workforce member, in the exercise of professional

judgment, determines that those requirements do not interfere with the ability to respond to the emergency circumstances.

e.When the Individual is Deceased

If the individual is deceased, a member of Cottonwood, Inc.'s workforce may disclose to a family member, or other person(s) identified who were involved in the individual's care or payment for health care prior to the individual's death, protected health information of the individual that is relevant to that person's involvement, unless doing so is inconsistent with any prior expressed preference of the individual that is known to COTTONWOOD, INC.

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 1, an authorized member of Cottonwood, Inc.'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 1.

When Cottonwood, Inc. is required by any of these situations to inform the individual of a use or disclosure permitted by relevant sections, Cottonwood, Inc.'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 Cottonwood, Inc.'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 and Security Policies. The use or disclosure should not occur until it has been approved by the Privacy Officer.

b.Permitted Uses and Disclosures

Cottonwood, Inc. 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.

Cottonwood, Inc. will meet the requirements of the following sections of these Privacy and Security Policies, as applicable, for uses and disclosures required by law:

(1)Section titled "Uses and Disclosures About Victims of Abuse, Neglect or Domestic Violence";

(2)Section titled "Disclosures for Judicial and Administrative Proceedings" ; and,

(3)Section titled "Disclosures for Law Enforcement Purposes".

3.Uses and Disclosures for Public Health Activities

a.Informing the Privacy Officer

Any member of Cottonwood, Inc.'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 and Security Policies. The use or disclosure should not occur until it has been approved by the Privacy Officer.

b.Permitted Disclosures

An authorized member of Cottonwood, Inc.'s workforce may use and 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 Cottonwood, Inc. 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)Cottonwood, Inc. 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)Cottonwood, Inc. 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.

(6)A school, about an individual who is a student or prospective student of the school if:

(a)The protected health information that is disclosed is limited to proof of immunization;

(b)The school is required by State or other law to have such proof of immunization prior to admitting the individual; and,

(c)Cottonwood, Inc. obtains the agreement to the disclosure from either:

i)A parent, guardian, or other person acting *in loco parentis* of the individual, if the individual is an unemancipated minor; or,

ii)The individual, if the individual is an adult or emancipated minor.

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

For purposes of reporting Abuse, Neglect, or Exploitation, which may involve disclosure of protected health information, see Policy 05-036.

5.Uses and Disclosures for Health Oversight Activities.

a.Delivery to Privacy Officer.

Any member of Cottonwood, Inc.'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 and Security Policies. The use or disclosure should not occur until it has been approved by the Privacy Officer.

b.General Rule.

An authorized member of Cottonwood, Inc.'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.Exception

For purposes of the disclosures permitted by "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 a patient's health is integral to the claim for public benefits or services.

d.Joint Activities or Investigations

Notwithstanding the exceptions stated 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 Cottonwood, Inc.'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 and Security Policies. The disclosure should not occur until it has been approved by the Privacy Officer.

b.General Rules

Cottonwood, Inc. 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 Cottonwood, Inc. 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)Cottonwood, Inc. 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)Cottonwood, Inc. 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, Cottonwood, Inc. 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 Cottonwood, Inc., 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. Cottonwood, Inc. will be considered to have received "satisfactory assurance" from a party seeking protected health information that the individual has received notice if Cottonwood, Inc. 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 Protected Order Sought. Cottonwood, Inc. will be considered to have received "satisfactory assurance" from a party seeking protected health information that a qualified protected order has been sought if Cottonwood, Inc. 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 protected 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 Cottonwood, Inc. 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 and Security Policies that otherwise permit or restrict uses or disclosures of protected health information.

7.Disclosures for Law Enforcement Purposes

a.Delivery to Privacy Officer

Any member of Cottonwood, Inc.'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 and Security 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 Cottonwood, Inc.'s workforce may disclose protected health information for a law enforcement purpose to a law enforcement official:

(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 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.

(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.

c.Limited Information for Identification and Location Purposes

Except for disclosures required by law as permitted by VII.G.7.b, above, an authorized member of Cottonwood, Inc.'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)Cottonwood, Inc. 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 or absence of facial hair (beard or moustache), scars, and tattoos.

(2)Except as stated in (1), above, a member of Cottonwood, Inc.'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 above, an authorized member of Cottonwood, Inc.'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 provision "Pursuant to Process and if Otherwise Required by Law" if:

(1)The individual agrees to the disclosure; or,

(2)Cottonwood, Inc. 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 Cottonwood, Inc., in the exercise of professional judgment.

e.Decedents

An authorized member of Cottonwood, Inc.'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 Cottonwood, Inc. has a suspicion that such death may have resulted from criminal conduct.

f.Crime on the Premises

An authorized member of Cottonwood, Inc.'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 Cottonwood, Inc.

g.Reporting Crime in Emergencies

If Cottonwood, Inc. is providing emergency health care in response to a medical emergency, other than on the premises of Cottonwood, Inc., an authorized member of Cottonwood, Inc.'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 Cottonwood, Inc.'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 Policy 05-036.

8.Uses and Disclosures About Decedents

a.Delivery to Privacy Officer

Any member of Cottonwood, Inc.'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 and Security 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 Cottonwood, Inc.'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 Cottonwood, Inc.'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, Cottonwood, Inc. 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 Cottonwood, Inc.'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 and Security 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 Cottonwood, Inc.'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 for Research Purposes

a.Delivery to Privacy Officer

Any member of Cottonwood, Inc.'s workforce who receives a request, or proposes, to use or disclose protected health information for research purposes 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 and Security 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 Cottonwood, Inc.'s workforce may use or disclose protected health information for research, regardless of the source of funding for the research, provided that:

(1)Board Approval of a Waiver of Authorization. Cottonwood, Inc. obtains documentation that an alteration to or waiver, in whole or in part, of the individual authorization required by these Privacy and Security Policies for use and disclosure of protected health information has been approved by either:

(a)An Institutional Review Board (IRB) established in accordance with the federal regulations set forth in the HIPAA Privacy Rule; or,

(b)A privacy board that meets the requirements of the HIPAA Privacy Rule, *see*, 45 CFR §164.512(i)(1)(i)(B).

The documentation must include all of the information required by the HIPAA Privacy Rule, *see*, 45 CFR

§164.512(i)(2).

(2)Reviews Preparatory to Research. Cottonwood, Inc. obtains from the researcher representations that:

(a)Use or disclosure is sought solely to review protected health information as necessary to prepare a research protocol or for similar purposes preparatory to research;

(b)No protected health information will be removed from Cottonwood, Inc. by the researcher in the course of the review; and,

(c)The protected health information for which use or access is sought is necessary for the research purposes.

(3)Research on Decedent's Information. Cottonwood, Inc. obtains from the researcher:

(a)Representation that the use or disclosure is sought solely for research on the protected health information of decedents;

(b)Documentation, at the request of Cottonwood, Inc., of the death of such individuals; and,

(c)Representation that the protected health information for which use or access is sought is necessary for the research purposes.

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

a.Delivery to Privacy Officer.

Any member of Cottonwood, Inc.'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 and Security 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 Cottonwood, Inc.'s workforce may,

consistent with applicable law and standards of ethical conduct, use or disclose protected health information, if the member of Cottonwood, Inc.'s workforce, in good faith, believes the use or disclosure meets either of the following:

(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 Cottonwood, Inc. 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 above, concerning a statement of an individual may not be made if the information described in that section is learned by Cottonwood, Inc.:

(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 above.

12.Uses and Disclosures for Specialized Government Functions.

a.Delivery to Privacy Officer.

Any member of Cottonwood, Inc.'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 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 and Security Policies. The use or disclosure may not occur until it has been approved by the Privacy Officer.

b.National Security and Intelligence Activities.

An authorized member of Cottonwood, Inc.'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.

c.Protective Services for the President and Others.

An authorized member of Cottonwood, Inc.'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 for the conduct of investigations authorized by 18 U.S.C. 871 and 879.

d.Correctional Institutions and Other Law Enforcement Custodial Situations

(1)Permitted Disclosures. An authorized member of Cottonwood, Inc.'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; or,

(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.

13.Disclosures for Workers' Compensation.

a.Permitted Disclosures.

An authorized member of Cottonwood, Inc.'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.

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

a.Delivery to Privacy Officer.

Any member of Cottonwood, Inc.'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 and Security 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, Cottonwood, Inc. 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 HIPAA. If the Secretary of Health and Human Services determines that exigent circumstances exist, such as when documents may be hidden or destroyed, Cottonwood, Inc. will

permit access by the Secretary of Health and Human Services at any time and without notice.

If any information required of Cottonwood, Inc. 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 Cottonwood, Inc. has made to obtain the information.

15.Disclosures by Whistleblowers.

A member of Cottonwood, Inc.'s workforce or a business associate may disclose protected heath information, provided that:

a.The workforce member or business associate believes in good faith that Cottonwood, Inc. has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services or conditions provided by Cottonwood, Inc. potentially endangers one or more individuals served or supported by Cottonwood, Inc., 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 Cottonwood, Inc. or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by Cottonwood, Inc.; 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.

16.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 or 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.

17.Disclosures to Business Associates.

a.Permitted Disclosures.

Authorized members of Cottonwood, Inc.'s workforce may disclose protected health information to a business associate and may allow a business associate to create, receive, maintain, or transmit protected health information on Cottonwood, Inc.'s behalf, if Cottonwood, Inc. has a written contract with the business associate that meets the requirements of the HIPAA Privacy Rule. However, such a written contract will not be required from a business associate that is a subcontractor of a business associate.

H.Uses and Disclosures for Marketing.

1.General Rule

As a rule, Cottonwood does not market third-party services or products to consumers.

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

I.Uses and Disclosures for Fundraising

1.General Rule

Any use of protected health information for the purpose of raising funds for Cottonwood's benefit will require authorization.

Opting Out

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

Cottonwood must make reasonable efforts to ensure that individuals who decide to opt out of receiving future fundraising communications are not sent future communications

J.Limited Data Set

1.General Rule

As a rule, Cottonwood does not foresee a circumstance where a limited data set may be used or disclosed.

K.Verification of Identity and Authority

1.General Rule

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

a.Except with respect to disclosures under "Uses and Disclosures Requiring an Opportunity for the Individual to Agree or to Object" of these Privacy and Security 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 and Security Policies, if the identity of that person is not known to Cottonwood, Inc.; 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 and Security Policies.

2.Personal Representatives

Unless the person and his or her authority is known to Cottonwood, Inc., the authorized member of Cottonwood, Inc.'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 and Security Policies on particular documentation, statements, or representations form the person requesting the protected health information, the authorized member of Cottonwood, Inc.'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 under "Disclosures for Law Enforcement Purposes" of these Privacy and Security 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.

b.The documentation required by "Board Approval of a Waiver of Authorization" of these privacy and security regulations, may be satisfied by one or more written statements provided that each is appropriately dated and signed in accordance with the HIPAA Privacy Rule, 45 CFR §164.512(i)(2)(i)&(v).

4.Identity of Public Officials

Cottonwood, Inc. 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 the 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

Cottonwood, Inc. 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

Staff will use professional judgment in verifying authority, identity and/or intent of the person requesting a disclosure.

L.Prior Authorizations

1.General Rule

Notwithstanding other sections of these Privacy and Security Policies, Cottonwood, Inc. may use or disclose protected health information, consistent with the below sections 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 consent by an Institutional Review Board.

2.Effect of Prior Authorization for Purposes Other Than Research

Notwithstanding any provisions of "Uses and Disclosures for Which an Authorization is Required" of these Privacy and Security Policies, Cottonwood, Inc. 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 "Right to Request Privacy Protection" of these Privacy and Security Policies.

3.Effect of Prior Permission for Research

Notwithstanding any provisions in "Uses and Disclosures for Which an Authorization is Required" of these Privacy and Security Policies and

section "Uses and Disclosures for Research Purposes" of these Privacy and Security Policies, Cottonwood, Inc. may, to the extent allowed by one of the following permissions, use or disclose, for research, protected health information that it created or received either before or after April 14, 2003, provided there is no agreed-to restriction in accordance with section "Right to Request Privacy Protection" of these Privacy and Security Policies, and Cottonwood, Inc. has obtained prior to April 14, 2003, either:

a. An authorization or other express legal permission from an individual to use or disclose protected health information for the research;

b. The informed consent of the individual to participate in the research; or,

c. A waiver, by an institutional Review Board, of informed consent for research in accordance with the requirements of the HIPAA Privacy Rule, *see*, 45 CFR §164.532(c)(3), provided that Cottonwood, Inc. must obtain authorization as required by "Uses and Disclosures for Which an Authorization is Required" of these Privacy and Security Policies, if, after April 14, 2003, informed consent is sought from an individual participating in the research.

VIII. RIGHTS OF INDIVIDUALS

A. Right to Request Privacy Protection

1. Restriction of Uses and Disclosures

a. Generally.

Cottonwood, Inc. will permit an individual to request that Cottonwood, Inc. 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 "Persons Involved in the Individual's Care; Notification" of these Privacy and Security Policies, for involvement in the individual's care and notification purposes.

b. Agreement to Restriction

With one exception, whether or not Cottonwood, Inc. will agree to the restriction will be determined by the Privacy Officer. The

exception is that Cottonwood, Inc. will always agree to a request of an individual to restrict disclosures of protected health information about the individual to a health plan if:

(1)The disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law; and,

(2)The protected health information pertains solely to a health care item or service for which the individual, or person other than the health plan on behalf of the individual, has paid Cottonwood, Inc. in full.

If a restriction is agreed to, a written or electronic record of that restriction shall be retained by Cottonwood, Inc. for six years from the date of its creation or the date when it was last in effect, whichever is later.

c.If Cottonwood, Inc. Agrees to a Restriction

If Cottonwood, Inc. 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 Cottonwood, Inc., or may be disclosed by an authorized member of Cottonwood, Inc.'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 Cottonwood, Inc.'s workforce making the disclosure shall request that health care provider not further use or disclose the information.

d.Limitations

A restriction agreed to by Cottonwood, Inc. under this section 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, "Right of Access");

(b)For facility directories pursuant to "Facility Directories"; or,

(c)When the use or disclosure does not require an authorization or opportunity to agree or object is not required, as in "Uses and Disclosures for which an Authorization or an Opportunity to Agree or Disagree is Not Required".

e.Termination of Restriction

Cottonwood, Inc. may terminate a restriction under this section, 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)Cottonwood, Inc. informs the individual that it is terminating its agreement to the restriction, except that such termination is:

(a)Not effective for protected health information restricted under the exception stated in "Agreement to Restriction," above; and,

(b)Only effective with respect to protected health information created or received after Cottonwood, Inc. has so informed the individual.

2.Restriction on Means and Location of Communications

a.Generally

Cottonwood, Inc. 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 Cottonwood, Inc. 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

Cottonwood, Inc.'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.

Cottonwood, Inc. 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

A consumer has the right of access to inspect and obtain a copy of protected health information about the consumer for as long as the protected health information is maintained, except for information compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative proceeding. The consumer must contact the case manager to arrange access. Cottonwood does not foresee not being able to give immediate access unless the disclosure would reveal a confidential source and/or increase the risk of harm to the consumer or others.

A reasonable, cost-based fee may be imposed for copies. The information will be provided in the form and format requested by the consumer, if it is readily producible. A summary of the requested information may be provided, if the consumer agrees to the summary.

1.Denial of Access

a.Unreviewable Grounds for Denial

Cottonwood, Inc. may deny an individual access without providing the individual an opportunity for review, in any of the following circumstances:

(1)Information Is Exempted. The protected health information is exempted from the right of access as stated in "Generally" of these Privacy and Security Policies.

(2)Inmates. When Cottonwood, Inc. is acting under the direction of a correctional institution, Cottonwood, Inc. 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)Research. An individual's access to protected health information created or obtained by Cottonwood, Inc. in the course of research that included treatment may be temporarily suspended for so long as the research is in progress, provided that the individual has agreed to the denial of access when consenting to participate in the research that includes treatment, and Cottonwood, Inc. has informed the individual that the right of access will be reinstated upon completion of the research.

(4)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

Cottonwood, Inc. may deny an individual access, provided that the individual is given a right to have the denial reviewed as stated in Section VIII.B.6.c, "Review of Denial", of these Privacy and Security 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.

2.Actions if Access is Denied

If consumer's access to protected health information is denied for the reasons stated above, in whole or in part, Cottonwood, will, to the extent possible, give the consumer access to any other protected health information requested, after excluding the denied protected health information.

Cottonwood shall provide a written denial to the consumer within the applicable time period. The denial shall contain:

a. The basis for the denial;
b. Of applicable, a statement of the individual's review rights, including a description of how the individual may exercise such review rights;

c. A description of how the individual may complain pursuant to Cottonwood's compliant procedures or to the Secretary of Health & Human Services, including the name or title, and the telephone number of the Cottonwood contact person or office designated to receive complaints;

If Cottonwood does not maintain the protected health information that is the subject of the individual's request for access, and Cottonwood knows where the requested information is maintained, a statement informing the individual where to direct the request for access.

3. If Cottonwood denies a consumer access to his or her protected health information, the consumer has a right to have the denial reviewed by a licensed health care professional who is designated by Cottonwood to act as a reviewing official and who did not participate in the original decision to deny, as long as the information requested is not considered "exempt".

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.

C.Right to Request Amendment

1.Generally

Except when access is denied under "Grounds for Denying the Amendment" of these Privacy and Security Policies, an individual shall have a right to have Cottonwood, Inc. 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 Case Manager, Director of Support Services, or the Director of CDDO Administration, and must state in the written request a reason to support the requested amendment. Individuals shall be informed in advance of these requirements in Cottonwood, Inc.'s Notice of Privacy Practices.

3.Action on Request for Amendment

a.Time Limits for Action

The designated staff shall act on a request for access no later than sixty (60) calendar days after Cottonwood, Inc.'s receipt of the request.

b.Inform Individual of Action on Request

If the request for amendment is accepted, in whole or in part, designated staff shall inform the individual of the acceptance of the request and make the amendment requested in accordance below, of these Privacy and Security Policies.

If the request for amendment is denied, in whole or in part, designated staff shall provide the individual with a written denial, in accordance with "Actions if Amendment is Denied" of these Privacy and Security Policies, and shall take the other actions required by that section.

4.Accepting the Amendment

If the individual's request for amendment is accepted, in whole or in part, designated staff shall:

a.Making the Amendment

Designated staff 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

Designated staff shall inform the individual as stated in "Inform Individual of Action on Request", that the amendment has been accepted and obtain the individual's identification of, and agreement to have Cottonwood, Inc. notify the relevant persons with the amendment needs to be shared in accordance with below.

c.Informing Others

Designated staff 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 Cottonwood, Inc. business associates, that Cottonwood, Inc. 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 designated staff determines that the protected health information or record that is the subject of the request:

a.Was not created by Cottonwood, Inc., 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; 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, Cottonwood, Inc. shall comply with the following:

a.Written Denial

Designated staff shall provide a written denial to the individual within the applicable time period stated in "Time Limits for Action" of these Privacy and Security 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 Cottonwood, Inc. 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 Cottonwood, Inc. pursuant to Cottonwood, Inc.'s complaint procedure or to the Secretary of Health and Human Services.

The description shall include the name or title and telephone number of the contact person or office designed by Cottonwood, Inc. 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. The written statement must be no more than one page.

c.Rebuttal Statement

The Privacy Officer may prepare, or cause to be prepared, a written rebuttal of Cottonwood, Inc. 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 Case Manager, Director of Support Services, or Director of CDDO Administration 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, Cottonwood, Inc.'s denial of the request, the individual's statement of disagreement, if any, and Cottonwood, Inc.'s rebuttal, if any, to the designated record set.

e.Future Disclosures

(1)If a statement of disagreement has been submitted by the individual, Cottonwood, Inc. will include the material appended in accordance with statements, 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, Cottonwood, Inc. 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 "Actions if Amendment is Denied" of these Privacy and Security 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, Cottonwood, Inc. shall separately transmit the material to the recipient of the transaction.

7.Documentation

The record of such designations described above will be maintained as incorporated in this policy.

D.Right to an Accounting of Disclosures

1.Right to Accounting

a.General Rule

Except as stated in "Exceptions" or "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 Cottonwood, Inc. 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 "Uses and Disclosures to Carry Out Treatment, Payment and Health Care Operations" of these Privacy and Security Policies;

(2)To individuals of protected health information about them;

(3)Incident to a use or disclosure otherwise permitted or required by these Privacy and Security Policies as provided in "Incidental Uses and Disclosures" of these Privacy and Security Policies;

(4)Pursuant to an authorization as provided in "Uses and Disclosures for Which an Authorization is Required";

(5)For the facility's directory or to persons involved in the individual's care or other notification purposes as provided in

"Uses and Disclosures Requiring an Opportunity for the Individual to Agree or Object";

(6)For national security or intelligence purposes as provided in "National Security and Intelligence Activities";

(7)To correctional institutions or law enforcement officials as provided in "Correctional Institutions and Other Law Enforcement Custodial Situations";

(8)As part of a limited data set in accordance with section "Limited Data Set"; 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 as described in "Uses and Disclosures for Health Oversight Activities" of these Privacy and Security Policies or to a law enforcement official as described in "Disclosures for Law Enforcement Purposes" shall be temporarily suspended for the time specified by the agency or official, if the agency or official provides Cottonwood, Inc. 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.Content

Except as otherwise stated in "Exceptions" of these Privacy and Security 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 Cottonwood, Inc.

b.Information

Except as stated in "Multiple Disclosures for a Single Purpose" or "Disclosures for Particular Research", 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 "Disclosure to the Secretary of Health and Human Services, if any; or,

(b)A copy of a written request for disclosure under "Uses and Disclosures for which an Authorization or an Opportunity to Agree or Object is Not Required", if any.

c.Multiple Disclosures for a Single Purpose

If, during the period covered by the accounting, Cottonwood, Inc. has made multiple disclosures of protected health information to the same person or entity for a single purpose under "Disclosure to the Secretary of Health and Human Services" or "Uses and Disclosures for which an Authorization or an Opportunity to Agree or Object is Not Required", the accounting may, with respect to such multiple disclosures, provide:

(1)The information required by above, 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.

d.Disclosures for Particular Research

If during the period covered by the accounting, Cottonwood, Inc. has made disclosures of protected information for a particular research purpose in accordance with "Uses and Disclosures for Research Purposes" of these Privacy and Security Policies for 50 or more individuals, the accounting may, with respect to the disclosures for which the protected health information about the individual may have been included, provide:

(1)The name of the protocol or other research activity;

(2)A description, in plain language, of the research protocol or other research activity, including the purpose of the research and the criteria for selecting particular records;

(3)A brief description of the type of protected health information that was disclosed;

(4)The date or period of time during which such disclosures occurred, or may have occurred, including the date of the last such disclosure during the accounting period;

(5)The name, address, and telephone number of the entity that sponsored the research and of the researcher to whom the information was disclosed; and,

(6)A statement that the protected health information of the individual may or may not have been disclosed for a particular protocol or other research activity.

If Cottonwood, Inc. provides an accounting for research disclosures in accordance with "Disclosures for Particular Research," and if it is reasonably likely that the protected health information of the individual was disclosed for that research protocol or activity, Cottonwood, Inc. shall, at the request of the individual, assist in contacting the entity that sponsored the research and the researcher.

3.Provision of the Accounting

a.Time Limit to Provide the Accounting

The Director of Support Services, Case Manager, Nurse Manager or Director of CDDO Administration shall act on a request for an accounting no later than sixty (60) calendar days after Cottonwood, Inc.'s receipt of the request.

Within that sixty (60) day period, the Director of Support Services, Case Manager, Nurse Manager or Director of CDDO Administration shall provide the individual with the accounting requested.

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 within the twelve (12) month period shall be as determined upon request and with advance notification in order to provide the individual an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

c.Documentation

The Privacy Officer shall document and retain the following:

(1)The information required to be included in an accounting under "Content of Accounting", 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 record of such designations will be maintained in the individual's file for at least six (6) years.

IX.PERSONAL REPRESENTATIVES

A.General Rule

Except as otherwise stated or permitted in these Privacy and Security Policies, Cottonwood, Inc. will treat a personal representative as the individual for purposes of these Privacy and Security 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, Cottonwood, Inc. 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, Cottonwood, Inc. 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 Cottonwood, Inc. and the minor with respect to such health care service.

2.**Exception.**

Notwithstanding the preceding paragraph "1. General Rule:"

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 "Right of Access" 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, Cottonwood, Inc. may not disclose, or provide access in accordance with "Right of Access" 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 as outlined in "Unemancipated Minors" and where there is no applicable access provision under State or other law, including case law, Cottonwood, Inc. may provide or deny access under "Right of Access" of these Privacy and Security 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, Cottonwood, Inc. will treat that person as a personal representative under these Privacy and Security 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 and Security Policies to the contrary, Cottonwood, Inc. may elect not to treat a person as the personal representative of an individual if:

1.Cottonwood, Inc. 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.Cottonwood, Inc., 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.

X.BREACH NOTIFICATION

A.Generally

Following discovery of a breach of unsecured protected health information,

Cottonwood, Inc.'s Privacy Officer shall notify each individual whose unsecured protected health information has been, or is reasonably believed by the Privacy Officer to have been, accessed, acquired, used, or disclosed as a result of that breach. Such notification shall be as stated in this Section 1.

B.Determining Whether a Breach Occurred

Unless the breach falls within the exceptions stated in subparagraphs 1, 2, or 3, of the definition of "breach", an acquisition, access, use, or disclosure of protected health information in a manner not permitted under the HIPAA Privacy Rule is presumed to be a breach unless the Security Officer or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

1.The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;

2.The unauthorized person who used the protected health information or to whom the disclosure was made;

3.Whether the protected health information was actually acquired or viewed; and,

4.The extent to which the risk to the protected health information has been mitigated.

C.When a Breach is Considered to be "Discovered"

A breach shall be considered to be "discovered" as of the first day on which the breach is known to Cottonwood, Inc., or, by exercising reasonable diligence would have been known to Cottonwood, Inc. Cottonwood, Inc. shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of Cottonwood, Inc.

D.Time of Notification

The notification to affected individuals shall be provided without unreasonable delay and in no case later than sixty (60) calendar days after discovery of the breach.

E.Content of Notification

The notification to affected individuals shall be written in plain language and include to the extent possible:

1.A brief description of what happened, including the date of the breach and

the date of the discovery of the breach, if known;

2.A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

3.Any steps individuals should take to protect themselves from potential harm resulting from the breach;

4.A brief description of what Cottonwood, Inc. is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and,

5.Contract procedures for individuals to ask questions or learn additional information, which shall include a toll-free number, an e-mail address, Web site, or postal address.

Generally, the notice should avoid including any sensitive material, such as the individual's actual social security number or credit card number.

As appropriate for the individuals to whom notice is given, reasonable steps shall be taken to have the notification translated into languages that are frequently encountered by Cottonwood, Inc. and as may be necessary to ensure effective communication with individuals with disabilities.

F.Methods of Notification

1.**Written Notice.** The notification to affected individuals shall be by first class mail to the individual at the last known address of the individual, or, if the individual has agreed to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as information is available.

If Cottonwood, Inc. knows the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification by first class mail to either the next of kin or the personal representative is permitted. It may be provided in one or more mailings as information is available.

2.**Substitute Notice**

a.**Generally.** If there is insufficient or out-of-date contact information that precludes written notification to the individual, a substitute form of notice, which is reasonably calculated to reach the individual, will be used. However, substitute notice will not be made if the insufficient or out-of-date contact information precludes written notice to the next of kin or personal representative.

b.**If Fewer Than 10 Individuals.** If there are fewer than ten (10) individuals to receive substitute notice, the substitute notice may be provided by an alternate form of written notice, telephone, or other means.

c.**If 10 or More Individuals.** If there are ten (10) or more individuals to receive substitute notice, then the substitute notice must:

(1)Be in the form of either: (a) a conspicuous posting for a period of ninety (90) days on the home page of the Web site of Cottonwood, Inc.; or, (b) a conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and,

(2)Include a toll-free telephone number that remains active for at least ninety (90) days where an individual can learn whether the individual's unsecured PHI may be included in the breach.

3.**Additional Notice in Urgent Situations.** If the Privacy Officer deems the situation to require urgency because of possible imminent misuse of unsecured protected health information, Cottonwood, Inc. may provide information to individuals by telephone or other means, as appropriate, in addition to the written notice stated above.

G.Notification to the Media

If a breach of unsecured protected health information involves more than five hundred (500) residents of a State or other jurisdiction, Cottonwood, Inc. shall notify prominent media outlets serving that State or jurisdiction of the breach. This notice will be provided without unreasonable delay and in no case later than sixty (60) calendar days after discovery of the breach. To the extent possible, the notification shall meet the requirements stated in "Content of Notification," for its content.

H.Notification to the Secretary of Health and Human Services

Following discovery of a breach, the Privacy Officer shall notify the Secretary of Health and Human Services as stated below.

1.**Breaches involving five hundred (500) or more individuals.** If the breach involves five hundred (500) or more individuals, with one exception, Cottonwood, Inc. will provide the Secretary of Health and Human Services with notice of the breach contemporaneously with its notice to the affected individuals. The notice will include the same information that is provided to affected individuals and will be provided to the Secretary of Health and

Human Services in the manner specified on the Health and Human Services Web site. The exception is when there is a law enforcement delay pursuant to "Enforcement Delay" of these Privacy and Security Policies.

2. **Breaches involving less than five hundred (500) individuals.** If the breach involves less than five hundred (500) individuals, the Privacy Officer will maintain a log or other documentation of such breaches and, no later than sixty (60) days after the end of each calendar year, provide the Secretary of Health and Human Services with notice of breaches discovered during the preceding calendar year in the manner specified on the Department of Health and Human Services Web site. This log will be kept for six years.

I. Notification from a Business Associate

When notification is received from a business associate of Cottonwood, Inc. of its discovery of a breach of unsecured protected health information, the Privacy Officer shall give notice to affected individuals in accordance with this Section 1 of these Privacy and Security Policies. Provided, however, if the agreement between Cottonwood, Inc. and the business associate permits, the Privacy Officer may require the business associate to give such notice.

J. Law Enforcement Delay

Notwithstanding anything in this "Breach Notification" to the contrary, if a law enforcement official states to Cottonwood, Inc. that a notification, notice, or posting required by "Breach Notification" would impede a criminal investigation or cause damage to national security, the Privacy Officer shall:

1. If the statement of the law enforcement official is in writing and specifies how long of a delay is required, delay the notification, notice, or posting for the time period specified in the writing; or,

2. If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily but no longer than 30 days from the date of the statement, unless a written statement as described in subparagraph 1, above, is submitted during that time.

Any member of the workforce of Cottonwood, Inc. who is contacted by a law enforcement official in this regard shall immediately refer the official to the Privacy Officer.

XI.POLICIES FOR THE SECURITY OF ELECTRONIC PROTECTED HEALTH INFORMATION

A.Administrative Safeguards

1.Security Management Process

The Security Officer shall oversee and be responsible for implementing procedures designed to prevent, detect, contain, and correct any security violations.

a.Risk Analysis

(1)Conducting Risk Analysis

The Security Officer shall ensure that Cottonwood, Inc. conducts an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.

(2)Documenting Risk Analysis

The Security Officer shall cause a copy of the risk analysis to be maintained in either written or electronic form for six (6) years from the date it was created or superseded by a newer analysis, whichever is later.

b.Risk Management

(1)Implementing Security Measures

The Security Officer shall implement security measures sufficient to reduce the risks and vulnerabilities identified in the risk analysis to a reasonable and appropriate level.

(2)Documentation of Security Measures

Cottonwood, Inc.'s Security Officer shall maintain, or cause to be maintained, a written or electronic record of the security measures. 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.

c.Sanction Policy

Any member of Cottonwood, Inc.'s workforce who fails to comply with Cottonwood, Inc.'s security policies and procedures or the

requirements of the HIPAA Security Rule shall be subject to sanctions imposed through Cottonwood, Inc.'s discipline and discharge policies.

Examples of the sanctions that may be applied for certain actions are stated in "Sanctions" of these Privacy and Security Policies.

d.**Information Systems Activity Review**

The Security Officer and designated IT staff shall regularly review records of the activity within Cottonwood, Inc.'s information systems. This review shall occur annually. As part of the review, the Security Officer shall review pertinent security logs and other documentation.

2.**Assigned Security Responsibility**

Cottonwood, Inc. shall designate a security official as stated in "Designation of Security Official" of these Privacy and Security Policies.

3.**Workforce Security**

Cottonwood, Inc. shall implement procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided in "Access Authorization" and "Access Establishment and Modification" of these Privacy and Security Policies. Furthermore, Cottonwood, Inc. shall implement procedures to ensure that workforce members who do not have access to electronic protected health information under "Information Access Management" of these Privacy and Security Policies from obtaining access to electronic protected health information.

a.**Authorization/Supervision of Workforce**

The Security Officer shall implement policies and procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in areas where electronic protected health information may be accessed.

Employees who have not been assigned a Cottonwood 'Master Key' are not authorized to be in an area where electronic protected health information may be accessed without supervision. Contracted cleaning personnel sign a confidentiality agreement assuring their understanding of privacy policies.

b.**Workforce Member Termination Procedures**

Reasonable to Implement: IT staff have enacted procedures

designed to ensure that, when a member of Cottonwood, Inc.'s workforce is separated from Cottonwood, Inc. for any reason whatsoever that person's access to electronic protected health information is foreclosed.

4.**Information Access Management**

a.**Minimum Necessary**

COTTONWOOD, INC. shall implement policies and procedures to authorize members of its workforce to access the minimum amount of electronic protected health information necessary to perform their job duties.

b.**Access Authorization**

The IT staff in concert with Management staff shall be responsible for implementing procedures for granting access to electronic protected health information. A workforce member's authorized access shall be based upon the minimum necessary informational needs of that employee, see, "Use and Disclosure of Only the Minimum Necessary".

c.**Access Establishment and Modification**

IT staff in concert with Management staff shall implement policies and procedures that, based upon Cottonwood, Inc.'s Access Authorization policies, establish, document, review, and modify a user's right of access to electronic protected health information. See Policy 02-021

IT staff shall ensure that the establishment of access for an employee, the review of the employee's access, and any modifications, are documented. This documentation shall be maintained for six years from the date of its creation or the date it was last in effect, whichever is later.

5.**Security Awareness and Training**

Cottonwood, Inc. shall provide regular training to its employees regarding information security and Cottonwood, Inc.'s policies and procedures. The Training Coordinator and Human Resources Assistant shall be responsible for designing and overseeing this training program.

a.**Security Reminders**

Based on its assessment of the risks and the nature of its work environment, Cottonwood, Inc., has determined that a security

reminder procedure is unnecessary.

b.**Protection Against Malicious Software**

IT staff shall implement procedures for guarding against, detecting and reporting malicious software.

IT staff shall ensure that all computers maintained by Cottonwood, Inc. have adequate virus protection software installed. IT staff shall ensure that all virus definitions are kept up to date and that all virus protection software has all current patches installed.

IT staff shall ensure that a firewall is installed between Cottonwood, Inc.'s network and the Internet. IT staff shall ensure the firewall is properly configured to allow Cottonwood, Inc.'s employees to use the Internet, in compliance with these policies and procedures, while denying unauthorized access from the internet

c.**Log-in monitoring**

IT staff shall enact a procedure to ensure the regular monitoring of log-in attempts. In the event IT staff discovers a discrepancy, IT staff shall notify the Security Officer who shall then take steps in accordance with "Security Incident Responses" of these Privacy and Security Policies.

d.**Password Management**

IT staff shall implement procedures for creating, changing and safeguarding passwords. See Policy 02-021

A valid password shall be determined periodically by the IT Department as per the current best practice.

6.**Security Incident Procedures**

a.**Security Incident Response and Reporting**

IT staff in concert with Management staff shall adopt procedures designed to identify and respond to suspected or known security incidents.

To the extent practicable, Cottonwood, Inc. shall take steps to mitigate any harmful effects of a security incident that are known to Cottonwood, Inc.

b.**Documentation of Security Incidents**

The Security Officer shall document, in written or electronic form, any security incidents and their outcomes.

The Security Officer shall ensure that documentation of any security incident is maintained for six (6) years from the date of the incident.

7.**Contingency Plan**

a.**Data Back-up Plan**

The IT staff will establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information. IT staff will also ensure that the electronic media containing these exact copies are stored in a secure manner.

b.**Disaster Recovery Plan**

The IT staff will establish and implement as needed procedures to restore any lost data from the exact copies created and stored pursuant to Cottonwood, Inc.'s Data Back-up Plan.

c.**Emergency Mode Operation Plan**

The CEO shall establish and implement as needed procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in an emergency mode. See ERT Plan.

d.**Testing and Revising the Contingency Plan**

The IT Department shall be responsible for overseeing an annual test of Cottonwood, Inc.'s contingency plan to be performed at the same time Cottonwood's Technology Plan is updated. Upon completion of the test, the IT Department shall review the results of the test and update the contingency plan as appropriate.

e.**Applications and Data Criticality Analysis**

After conducting a thorough assessment of all relevant factors, including those outlined by Health and Human Services in the HIPAA Security Rule, Cottonwood, Inc. has determined that performing an Applications and Data Criticality Analysis is not reasonable in its work environment.

8.**Evaluation**

The CFO shall be responsible for the performance of periodic evaluations both technical and non-technical to ensure that Cottonwood, Inc.'s Security

Policies and Procedures meet and continue to meet the requirements of the HIPAA Security Rule in light of both environmental and operational changes.

If, after this evaluation, the CFO determines that Cottonwood, Inc.'s security policies do not meet the requirements of the HIPAA Security Rule, the Security Officer shall revise Cottonwood, Inc.'s Security Policies and Procedures as necessary to ensure they meet the requirements of the HIPAA Security Rule.

9.**Business Associates**

Prior to Cottonwood, Inc. disclosing any electronic protected health information to a business associate or allowing a business associate to create or receive electronic protected health information on its behalf, Cottonwood, Inc. shall comply with Business Associate Section of these Privacy and Security Policies.

B.Physical Safeguards

Cottonwood, Inc. shall implement physical measures designed to protect its information systems and facilities from unauthorized entry, natural disasters, and environmental hazards. See ERT Plan.

1.**Facility Access Controls**

Cottonwood, Inc. shall implement procedures to ensure that unauthorized physical access to its electronic information systems and the facilities in which they are housed is limited while ensuring that properly authorized access is allowed.

a.**Contingency Operations**

Cottonwood, Inc. shall establish procedures that, in the event of emergency, allow members of Cottonwood, Inc.'s workforce to access its facilities in support of restoration of lost data under Cottonwood, Inc.'s disaster recovery and emergency mode operations plans.

b.**Facility Security Plan**

Cottonwood, Inc. shall implement procedures designed to safeguard its facility (facilities) and the equipment stored therein from unauthorized physical access, tampering, and theft.

c.**Access Control and Validation Procedures**

Cottonwood management shall implement procedures to control and validate individual's access to facilities based on their role or

function. These procedures shall include procedures for visitor control and controlling access to software programs for testing and revision. See Policy & Procedure Manual.

d. **Maintenance Records**

After conducting a thorough assessment of all relevant factors, including those outlined by Health and Human Services in the HIPAA Security Rule, Cottonwood, Inc. has determined that maintaining financial vendor records is an appropriate alternative measure.

2. **Workstation Use**

In order to ensure the security of electronic protected health information, physical safeguards shall be implemented for all of Cottonwood, Inc.'s workstations that can access electronic protected health information. The Security Officer shall design and implement procedures that govern the operation of desktop, laptop, handheld and any other types of workstations that can access electronic protected health information.

These procedures shall describe the appropriate functions to be performed by a workstation, the manner in which those functions are to be performed, and the physical attributes or the surroundings of workstations that can access electronic protected health information.

All of Cottonwood, Inc.'s workstations that can access electronic protected health information shall be operated in accordance with the workstation use procedures developed in accordance with this policy. Violations of these procedures will be sanctioned according to the Sanctions policy outlined in these Privacy and Security Policies. See also Policy 02-021.

3. **Workstation Security**

Cottonwood, Inc. shall implement physical safeguards for all workstations that access electronic protected health information in order to restrict access to authorized users.

4. **Device and Media Controls**

Cottonwood, Inc. shall implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of Cottonwood, Inc.'s facility. Cottonwood, Inc. shall also implement policies and procedure that govern the movement of these items within its facility.

a.**Disposal**

When a member of Cottonwood, Inc., Inc.'s workforce disposes of computer hardware or other electronic media containing electronic protected health information, the Security Officer shall ensure that Cottonwood, Inc.'s procedure for the removal of electronic protected health information is followed. These procedures are outlined in Policy 02-021.

b.**Media Re-Use**

Members of Cottonwood, Inc.'s workforce, who use re-usable electronic media, shall follow procedures outlined in Policy 02-021.

c.**Accountability**

After conducting a thorough assessment of all relevant factors, including those outlined by Health and Human Services in the HIPAA Security Rule, Cottonwood, Inc. has determined that an accountability policy is not reasonable in its work environment.

d.**Data Back-up and Storage**

After conducting a thorough assessment of all relevant factors, including those outlined by Health and Human Services in the HIPAA Security Rule, Cottonwood, Inc. has determined that a formal Data Back-up and Storage policy and procedure is not reasonable in its work environment.

Instead, as a reasonable equivalent alternative, Cottonwood, Inc. will rely upon the retrievable exact copies created as part of its routine back-up. In the event of loss of electronic protected health information due to a move of equipment, Cottonwood, Inc. will restore the lost information from Cottonwood, Inc.'s regularly performed back-up.

C.Technical Safeguards

Cottonwood, Inc. will implement policies and procedures for the use of technology in protecting electronic protected health information and for controlling access to electronic protected health information.

1.**Access Control**

Cottonwood, Inc. will deploy technology and implement policies and procedures governing the use of this technology for information systems that contain electronic protected health information to ensure that only those persons or software programs that have been granted access rights pursuant

to Cottonwood, Inc.'s Policies concerning Information Access Management, are able to access electronic protected health information.

a.**Unique User Identification**

Each user that has been authorized to access information systems which contain electronic protected health information or from which electronic protected health information can be accessed shall be assigned a unique name and/or number for identifying the user to system and for tracking the users movements within the system.

b.**Emergency Access Procedure**

The Security Officer shall establish and implement procedures for obtaining necessary electronic protected health information during an emergency.

c.**Automatic Logoff**

The Security Officer shall implement electronic procedures to ensure that electronic sessions terminate after a period of inactivity. See Policy 02-021

d.**Encryption and Decryption**

Cottonwood, Inc. shall implement a mechanism to encrypt and decrypt electronic protected health information under certain circumstances. See Policy 02-021.

2.**Audit Controls**

The Security Officer shall ensure that hardware, software, or procedural mechanisms are implemented in order to record and examine activity in Cottonwood, Inc.'s information systems that contain or use electronic protected health information. Logs are an integral component of Cottonwood's network software. Audits will be performed on a case by case basis.

3.**Integrity of Electronic Protected Health Information**

Cottonwood, Inc. shall implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

a.**Mechanism to Authenticate Electronic Protected Health Information**

The Security Officer shall ensure that technical mechanisms to corroborate

that electronic protected health information has not been altered or destroyed in an unauthorized manner. "Read Only" designations are determined by content by the initiator of the file.

4.**Person or Entity Authentication**

Human Resources shall implement procedures to verify that a person or entity seeking access to electronic protected health information is the person or entity claimed.

5.**Transmission Security**

Cottonwood, Inc. shall implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

a.**Integrity Controls**

The Security Officer shall implement technical security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until Cottonwood, Inc. disposes of it.

b.**Encryption**

The Security Officer shall implement a mechanism to encrypt electronic protected health information whenever he or she deems it to be appropriate.

XII.DEFINITIONS

As used in these Privacy and Security Policy, the following terms and phrases shall have the following meanings.

A.Access

"Access" means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.

B.Administrative Safeguards

"Administrative safeguards" are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of Cottonwood, Inc.'s workforce in relation to the protection of that information.

C.Authentication

"Authentication" means the corroboration that a person is the one claimed.

D.Authorized Member of Cottonwood, Inc.'s Workforce

"Authorized member of Cottonwood, Inc.'s workforce" means a member of Cottonwood, Inc.'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 Security Officer; or, (c) by the Privacy Officer or Security Officer.

E.Availability

"Availability" means the property that data or information is accessible and useable upon demand by an authorized person.

F.Breach

"Breach" means the acquisition, access, use or disclosure of protected health information in a manner not permitted by the HIPAA Privacy Rule which compromises the security or privacy of the protected health information. Provided, however, breach does not include:

1.Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of Cottonwood, Inc. or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted by the HIPAA Privacy Rule.

2.Any inadvertent disclosure by a person who is authorized to access protected health information at Cottonwood, Inc. or business associate to another person authorized to access protected health information at the same Cottonwood, Inc. or business associate in which Cottonwood, Inc. participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the HIPAA Privacy Rule.

3.A disclosure of protected health information where Cottonwood, Inc. or a business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

G.Business Associate

"Business associate" means:

1.Except as provided in paragraph (4) of this definition, business associate means, with respect to Cottonwood, Inc., a person who:

a.On behalf of Cottonwood, Inc., but other than in the capacity of a member of Cottonwood, Inc.'s workforce, creates, receives, maintains, or transmits protected health information for a function or activity regulated by the HIPAA regulations, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and repricing, or

b.Provides, other than in the capacity of a member of Cottonwood, Inc.'s workforce, legal, actuarial, accounting, consulting, data aggregation (as defined in the Privacy Rule), management, administrative, accreditation, or financial services to or for Cottonwood, Inc., where the provision of the service involves the disclosure of protected health information from Cottonwood, Inc. to the person.

2.A covered entity may be a business associate of another covered entity.

3.Business associate includes:

a.A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to Cottonwood, Inc. and that requires access on a routine basis to such protected health information.

b.A person that offers a personal health record to one or more individuals on behalf of Cottonwood, Inc.

c.A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of a business associate.

4.Business associate does not include:

a.A health care provider, with respect to disclosures by a covered entity to the health care provider concerning the treatment of the individual.

b.A plan sponsor, with respect to disclosures by a group health plan (or by a health insurance issuer or HMO) with respect to a group health plan) to the plan sponsor, to the extent that requirements of HIPAA apply and are met.

c.A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or

collecting protected health information for such purposes, to the extent such activities are authorized by law.

H.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.

I.Designated Record Set

"Designated record set" means a group of records maintained by or for Cottonwood, Inc. that is:

1.The medical records and billing records about individuals maintained by or for Cottonwood, Inc.;

2.The enrollment, payment, claims adjudication, and case or medical management record systems maintained for a health plan; or,

3.Used, in whole or in part, by or for Cottonwood, Inc. 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 Cottonwood, Inc.

J.Disclosure

"Disclosure" means the release, transfer, provision of access to, or divulging in any other manner of information outside Cottonwood, Inc.

K.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.

L.Health Care Operations

"Health care operations" means any of the following activities of Cottonwood, Inc. 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; patient safety activities (as defined in 42 CFR 3.20); population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; 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.Except as prohibited for genetic information, underwriting, enrollment, premium rating, and other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided the requirements of the HIPAA Privacy Rule concerning uses and disclosures for underwriting and related purposes are met, if applicable, see, *45 CFR §164.514(g)*.

4.Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;

5.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,

6.Business management and general administrative activities of Cottonwood, Inc., including, but not limited to:

a.Management activities relating to implementation of and compliance with the requirements of these Privacy and Security 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 Cottonwood, Inc. 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", creating de-identified health information or a limited data set, and fundraising for the benefit of Cottonwood, Inc.

M.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.

N.HIPAA Breach Notification Rule

"HIPAA Breach Notification Rule" means 45 CFR Subpart D, as amended from time to time.

O.HIPAA Privacy Rule

"HIPAA Privacy Rule" means 45 CFR Subpart E, as amended from time to time.

P.HIPAA Security Rule

"HIPAA Security Rule" means 45 CFR Subpart C, as amended from time to time.

Q.Information System

"Information system" means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

R.Inmate

"Inmate" means a person incarcerated in or otherwise confined to a correctional

institution.

S.Integrity

"Integrity" means the property that data or information have not been altered or destroyed in an unauthorized manner.

T.Law Enforcement Official

"Law enforcement official" means an officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or 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."

U.Malicious Software

"Malicious Software" means software, for example, a virus, designed to damage or disrupt a system.

V.Password

"Password" means confidential authentication information composed of a string of characters.

W.Payment

"Payment" means the activities undertaken by Cottonwood, Inc. 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 Cottonwood, Inc.

X.Physical Safeguards

"Physical safeguards" are physical measures, policies, and procedures to protect Cottonwood, Inc.'s electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

Y.Privacy Officer

"Privacy Officer" is the member of Cottonwood, Inc.'s workforce who has been designated, pursuant to the HIPAA Privacy Rule, with responsibility for ensuring Cottonwood, Inc.'s compliance with the HIPAA Privacy Rule.

AA. 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.

BB. Security Officer

"Security Officer" is the member as Cottonwood, Inc.'s workforce who has been designated, pursuant to the HIPAA Security Rule, with responsibility for the development, updating and implementation of Cottonwood, Inc.'s security policies.

CC. Security or Security Measures

"Security or Security Measures" encompass all of the administrative, physical, and technical safeguards in an information system.

DD. Security Incident

"Security incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

EE. Technical Safeguards

"Technical safeguards" means the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.

FF. These Privacy and Security Policies

"These Privacy and Security Policies" means these Privacy and Security Policies adopted by Cottonwood, Inc. concerning the protection of the privacy and security of protected health information.

GG. 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 a patient; or the referral of a patient for health care from one health care provider to another.

HH. Unsecured Protected Health Information

"Unsecured protected health information" means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of technology or methodology specified by the Secretary of the U.S. Department of Health and Human Services (the "Secretary of Health and Human Services") through guidance issued by the Secretary of Health and Human Services on the Health and Human Services Web site.

II. Use

"Use" means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of that information within Cottonwood, Inc.

JJ. Workforce

"Workforce" means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for Cottonwood, Inc., is under the direct control of Cottonwood, Inc., whether or not they are paid by Cottonwood, Inc.

APPENDIX A

Identification of Workforce Members' Access To Protected Health Information.

(1) Director/Management Team:

The Administrator/Executive Director must have access to all protected health information maintained by the Cottonwood. There are no conditions applicable to that access. For the CDDO staff/function, access would be area wide.

(2) Clinic Staff:

Clinic staff must have access to all clinical information of individuals to whom he/she is providing services. There are no conditions applicable to that access. He/she must have access to billing information concerning an individual if the Billing Staff must discuss billing matters concerning that individual with the clinic staff.

(3) Direct Support Staff:

Direct Support Staff must have access to all health/clinical information of the individuals for who he/she supports, necessary to perform their responsibilities. There are no conditions applicable to that access.

(4) Billing Staff/Finance Manager:

The Billing Staff must have access to all billing and payment information concerning the individual. There are no conditions applicable to that access. He/She must have access to health/clinical information concerning the individual to the extent necessary to bill for services provided to the individual.

(5) Front Office Staff:

The Front Office Staff must have access to information necessary for the support role that he/she provides.

(6) Janitorial/Maintenance/HR Assistant/Marketing/Sales/Temporary Workers/Shipping and Receiving Staff:

This category of staff does not need access to any protected health information concerning any individual of Cottonwood.

(7) Management Information Staff:

The Management Information staff will have access to all electronic information as a function of the system management.

(8) Mid-Management Staff Coordinators:

Mid-management staff will have access to all protected health information for individuals whom he/she supports. For CDDO-related staff/functions, access would be area wide.

(9) Human Rights Committee Members:

Due to oversight roles as assigned by state regulations, volunteer committee members have access to protected health information.

(10) Board of Trustees Members:

Board of Trustees may see incidental protected health information if necessary to perform their governance role.