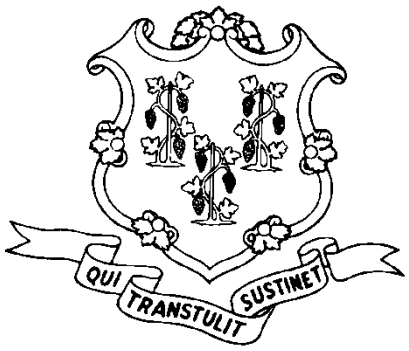
State of Connecticut
Department of Social Services

HIPAA Policies and Procedures Manual



Updated 9/17/13

Overview As of April 14, 2003, the State of Connecticut Department of Social Services (DSS) is required by federal law to comply with the Privacy Rule contained in a federal law called HIPAA (Health Insurance Portability and Accountability Act). Although HIPAA's Privacy Rule did not change many of DSS' practices because DSS was already subject to extensive state and federal laws governing privacy and confidentiality, there were some important changes that became mandated by the new law.

Effective February 17, 2010, new federal requirements required DSS to inform individuals if there has been a breach of unsecured protected health information. Policies and procedures related to these federal requirements are located in section IV of this manual.

New regulations modifying the privacy and breach notification requirements under HIPAA became effective September 23, 2013, and are incorporated into this Manual.

Table of Contents

HIPAA Privacy Rule Definitions

The Privacy Rule contains many specialized terms and definitions. This glossary defines the some of the terms that are used in the Privacy Rule.

Accounting of Disclosures- A disclosure is a release of information outside of the Department. The Department is required to keep a history of when and to whom protected health information (PHI) is disclosed if the disclosure occurs outside the scope of treatment, payment, and health care operations, and is not specifically authorized by the patient. A person has a right to receive an accounting of disclosures of PHI made by the Department in the six years prior to the date of the request for an accounting, although the Department is not required to begin tracking disclosures until April 14, 2003.

Authorization- An authorization is a specific written document signed by a client that gives the Department permission to use or disclose PHI for purposes other than treatment, payment and health care operations.

Business Associate (BA)- A business associate is a person or organization who, on behalf of the covered entity and not as a member of the covered entity's work force, creates, receives, maintains or transmits PHI for a function or activity regulated by HIPAA, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, and billing. A business associate is also a person or organization, other than a member of the covered entity's workforce, provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for the covered entity where the provision of the service involves the disclosure of PHI from the covered entity or from another business associate of the covered entity to the person or organization. A health care provider is not a business associate of the Department.

Confidential (Alternative) Communication Restrictions- According to the Privacy Rule, the Department must permit and accommodate reasonable requests for confidential communication of PHI, if the individual clearly states that the disclosure of all or part of that information could endanger the individual.

For example, a client may request that any or all notices from the Department be sent to an alternative address, such as a work address or a PO Box.

De-identified Information- De-identified information is health information that does not specifically identify an individual and there is no reasonable basis to believe that the information alone *could* be used to identify an individual. De-identified information is not individually identifiable health information. In order to be considered de-identified, the following 18 elements must be removed: name; address; names of relatives; names of employers; birth date; telephone number; fax number; e-mail addresses; social security number; medical record number; health plan beneficiary number; account number; certificate/license number; any vehicle or device serial number; web URL; Internet Protocol Address; Finger or voice prints; Photographic images (e.g. full facial photographs); and any other unique identifying number, characteristic, or code. Information may also be statistically de-identified. This is typically performed by an experienced statistician who analyzes the data and affirms that the risk is "very small" that a particular person could be identified from the information collected.

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

Family Member - include parents, spouses, siblings, and children; grandparents, grandchildren, aunts, uncles, nephews, and nieces. great-grandparents, great-grandchildren, great aunts, great uncles, and first cousins great-great grandparents, great-great grandchildren, and children of first cousins. Relatives by less than full consanguinity

(such as half- siblings, who share only one parent) are treated the same as relatives by full consanguinity (such as siblings who share both parents).

Individual- The person who is the subject of the PHI.

Individually Identifiable Health Information – is information that is a subset of health information, including demographic information collected from an individual, and: (1) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) related to the past, present of future physical or mental health of condition of an individual; the provision of health care to an individual; or the past, present of future payment for the provision of health care to an individual and (i) that identifies the individual or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Minimum Necessary- When using, disclosing, or requesting PHI, the Department must make reasonable efforts to limit the information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. This applies not only when we respond to requests for PHI, but also when we request PHI from other entities.

Notice of Privacy Practices- The notice of privacy practices describes how the Department uses and discloses PHI and describes the clients' rights regarding the use and disclosure of their PHI. The Department sends to every client receiving health benefits paid for by the Department at the initial grant of benefits and at each yearly redetermination. The Notice of Privacy Practices is available at all of the Departments' offices and on the Department's website.

Personal Representative- A personal representative is a person who has been appointed to act on behalf of the individual in making health care related decisions. In general, the scope of the personal representative's authority to act for the individual under the Privacy Rule derives from his or her authority under applicable law to make health care decisions for the individual. Where the person has broad authority to act on the behalf of a living individual in making decisions related to health care, such as a parent with respect to a minor child or a legal guardian of a mentally incompetent adult, the Department must treat the personal representative as the individual for all purposes under the Rule, unless an exception applies. In Connecticut, personal representatives include powers of attorney, conservators of person or estate and legal guardians.

Protected Health Information (PHI) - PHI is individually identifiable health information that is transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium. PHI excludes individually identifiable health information in education and other records covered by the Family Education Rights and Privacy Act, as amended, 20 USC 1232g (FERPA); in employment records held by a covered entity in its role as an employer; and regarding a person who has been deceased for more than 50 years.

Psychotherapy Notes - *Psychotherapy notes* means notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. *Psychotherapy notes* excludes medication prescription
and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: Diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

Treatment, Payment and Health Care Operations (TPO) - For the Department, treatment, payment, and operations include the following activities:

Treatment – Provision, coordination, or management of health care and related services by one or more health care providers, including but not limited to

- The coordination or management of health care between a health care provider and a third party;
- Consultation between health care providers relating to a client;
- The referral of a client for health care from one health care provider to another.

Payment - Activities undertaken by the Department to obtain reimbursement for the provision of health care, including but not limited to:

- Determination of eligibility or coverage (including the coordination of benefits) and claim adjudication;
- Risk adjustments;
- Billing;
- Claims management;
- Collection activities;
- Medical necessity review and/or justification of charges;
- Utilization review activities;
- Disclosure to consumer reporting agencies relating to collection of premiums or reimbursement.

Health Care Operations - The Department's necessary administrative, business, and education functions, including but not limited to:

- Quality assessment and improvement activities, but not limited to 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;
- Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, and 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 skill as health care providers;
- Conducting training;
- Accreditation activities;
- Certification, licensing, or credentialing activities;
- Insurance activities relating to the renewal or replacement of a contract for health insurance or health benefits;
- Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
- The Department's business planning and development;
- The Department's business management and administration activities.

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

Workforce means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate.

Section I – Individual Rights

A. Access of individuals to PHI (45 C.F.R. 164.524; UPM 1020.10)

General

POLICY 100: The Department permits an individual to request access to, inspect or obtain a copy of, the PHI about the individual that is maintained in the individual's record and the Department must grant or deny said request.

Procedures:

The Department requires that all requests for access to PHI be made in writing. The Department must act on a request for access no later than 30 days after receipt of the request as follows:

If the Department grants the request, in whole or in part, the Department must inform the person that the request is accepted and provide the access requested. If the Department denies the request, in whole or in part, it must provide the person with a written denial.

If the Department is unable to grant or deny a request within the 30-day period, the Department may extend the time for taking such action by not more than 30 days if the Department provides a written statement to the individual, stating the reasons for the delay and the date by which the Department will complete its action on the request. The Department may have only one such extension.

Limitations to access

POLICY 102: Individuals have the right of access to inspect and obtain a copy of the PHI that is in their records for as long as the PHI is maintained in the record, except that individuals do not have the right of access to:

- Psychotherapy notes;
- The names of individuals who have disclosed information about the individual without the individual's knowledge under a promise of confidentiality;
- Information compiled in reasonable anticipation of, for use in, a civil or criminal proceeding; and
- Medical, psychiatric or psychological data concerning the individual if a licensed health professional has determined that access requested is reasonably likely to endanger the life or physical safety of the individual.

Denial of access

General

POLICY 104: The Department may deny an individual access to records in accordance with the above.

Procedures:

The Department will inform individuals who have been denied access to their records for any reason, that they have the right to petition the Superior Court for an order requiring the agency to grant them access to the PHI within thirty (30) days of the denial of access.

If the Department denies individuals requests for access, it must provide individuals with a written denial, in plain language. The written denial must be issued no later than 30 days or 60 days after receipt of the request (see policy 100 above). It must contain:

- The basis for the denial;
- As applicable, a statement of the individual's review rights, including how the person may exercise such review rights; and
- A description of how the individual may complain to the Department or to the Secretary of Health and Human Services (See Policy and Procedures Section III D, Complaints to the Department and Secretary of Health and Human Services regarding how to file a complaint with the Department or to the Secretary of Health and Human Services).

Without a right to review

POLICY 106: The Department may deny an individual or an individual's personal representative access to psychotherapy notes; information compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative action; or PHI that 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. , The individual or the individual's personal representative does not have the right to have the denial reviewed.

With a right of review

POLICY 108: If the Department denies access to an individual or an individual's personal representative because a licensed health care professional has determined, in the exercise of professional judgment, that medical, psychiatric or psychological data requested is reasonably likely to endanger the life or physical safety of the individual, the individual or the individual's personal representative has the right to have the denial reviewed.

Procedures:

If the individual requests, in writing, a review of the denial of access, the Department will designate a licensed health care professional who was not directly involved in the denial to review the decision to deny access.

The Department will promptly refer such request for review to such designated reviewing professional. The reviewing professional must determine, within a reasonable period of time, whether or not to deny access.

Once that determination is made, the Department must promptly provide written notice to the individual of the determination of the designated reviewing professional and take the action to carry out the determination.

Granting access to PHI

POLICY 110: If the Department grants the individual's request for access to PHI in his or her record, either in the form of inspection or a copy, or both, the Department will inform the individual that the request has been granted and provide the requested access in a timely manner, i.e., no later than 30 days or 60 after receipt of the request (see policy 100 above).

Procedures:

The Department will arrange with the individual a convenient time and place to inspect or obtain a copy of the PHI or mail a copy of the PHI at the individual's request.

As necessary, the Department will discuss the scope, format or other aspects of the request for access with the individual, to facilitate the timely provision of access.

POLICY 112: The Department will provide the individual with access to the PHI in the form or format requested by the individual, if it is readily producible in such form or format; or if not, the PHI will be provided to the individual in a readable hard copy form or such other form and format as agreed to by the Department and the individual.

Procedures:

If the same PHI that is the subject of the request for access is maintained in more than one record or at more than one location, the Department need only produce the PHI once in response to a request for access.

The Department will not impose fees on individuals requesting access to their own PHI.

POLICY 114: Notwithstanding Policy 112, if the PHI requested for access is maintained in one or more records electronically and if the individual requests an electronic copy of such information, the Department must provide the individual with access to the PHI in the electronic form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by the Department and the individual.

POLICY 116: If an individual's request for access directs the Department to transmit a copy of the PHI or other aspects of the record directly to another person who the individual designates, the Department must provide the copy to the person designated by the individual.

Procedure:

The individual's request must be writing, signed by the individual, and it must clearly identify the designated person and where to send the copy of the PHI.

Informing the individual of location of documents

POLICY 118: If the Department does not maintain the PHI that is the subject of the individual's request for access and the Department knows where the PHI is maintained, the Department must inform the individual where to direct the request for access.

Documentation of records requested

POLICY 120: The Department will document the records that were requested to be accessed by individuals and such documentation will be maintained in accordance with Policy 352.

Documentation of persons processing access requests

POLICY 122: The Department will document the titles of the persons or offices responsible for receiving and processing requests for access by individuals and such documentation will be maintained in accordance with Policy 352.

B. Amendment of PHI (45 C.F.R. 164.526)

General

POLICY 124: In accordance with the policies set forth below, an individual has the right to have the Department amend PHI contained in the individual's record for as long as the PHI is maintained in the record.

Procedures:

The Department will inform individuals that requests to amend PHI must be in writing and that they must provide a reason to support the requested amendment.

The Department will act on the individual's request to amend PHI no later than 60 days after receipt of the request.

If the Department is unable to grant or deny the request within the 60-day period, the Department may extend the time for taking such action by not more than 30 days if the Department provides a written statement to the individual indicating the reasons for the delay and the date by which the Department will complete its action on the request. The Department may have only one such extension.

Granting the amendment

POLICY 126: The Department may grant the individual's request to amend PHI, in whole or in part.

Procedure

If the Department accepts the requested amendment, in whole or in part, it will take the following actions:

- Document in the individual's record that the request to amend the record is granted.
- Make the appropriate amendment to the PHI or record that is the subject of the request for the amendment, by, at a minimum, identifying the record that is affected by the amendment and appending or providing a link to the location of the amendment;
- Inform the individual, in writing, no later than 60 days after receipt of the request for the amendment, that the amendment is accepted. If the Department cannot grant the amendment within that time, it may extend the time in accordance with Policy 100, and request and obtain the individual's identification of an agreement to notify relevant person(s) with whom the amendment needs to be shared. Toward that end, the Department will make reasonable efforts to inform, and provide the amendment within a reasonable time to:
  - Persons identified by the individual as having received PHI about the individual and needing the amendment; and
  - Persons, including business associates, the Department knows have the PHI that is the subject of the amendment and that may have relied, or could foreseeably rely, on such information to the detriment of the individual.

POLICY 128: When the Department is informed by another covered entity of an amendment to an individual's PHI, the Department will amend the PHI in its records by identifying the record that is affected by the amendment and appending or providing a link to the amendment.

Denial of a request to amend

POLICY 130: The Department may deny an individual's request to amend PHI under the following circumstances:

- the record was not created by the Department, unless the individual provides a reasonable basis to believe that the originator of the PHI is no longer available to act on the requested amendment;
- the PHI is not part of the record;
- the record is not available for inspection under the provisions for access to records (See Policy 102); or
- the record maintained by the Department is accurate and complete.

Procedures:

If the Department denies the requested amendment, in whole or in part, the Department will provide the individual with a written denial no later than 60 days after receipt of the request. If the Department is unable to issue the denial within this time, the Department may extend the time in accordance with Policy 100.

The written denial will be in plain language and will state

- the basis of the denial, in accordance with one of the bases stated above;
- the individual's right to submit a written statement disagreeing with

denial and how to file the statement;

- that if the individual does not submit a statement of disagreement, the individual may request that the Department provide the individual's request for amendment and the denial with any future disclosures of the PHI that is the subject of the amendment;
- a description of how the individual may make a complaint to the Department or to the Secretary of Health and Human Services, in accordance with complaint procedures set forth in the Privacy Rule and these Policies and Procedures (See Policy 328); and
- the description will include the name or title and telephone number of the Privacy Officer.

Statement of disagreement and rebuttal

POLICY 132: The Department will permit the individual to submit a written statement disagreeing with its denial of a requested amendment and stating the basis for the disagreement and the Department may prepare a written rebuttal to the statement of disagreement.

Procedures:

The Privacy Officer will review the individual's written statement and place it in the individual's record.

The Department may prepare a written rebuttal to the disagreement statement provided by the individual and provide a copy of such rebuttal to the individual who submitted the request to amend.

The Department will identify, by noting in the record, the PHI that is the subject of the disputed amendment and append to the record the individual's request for amendment, the Department's denial of the request for amendment, the individual's statement of disagreement and, if any, the Department's rebuttal.

Subsequent disclosures

POLICY 134: If an individual has submitted a statement of disagreement, the Department will include, in any subsequent disclosures of the PHI to which the disagreement relates, all of the items set forth above, i.e., the individual's request for amendment, the Department's denial of the request, the statement of disagreement, and, if any, the Department's rebuttal.

If an individual has <u>not</u> submitted a statement of disagreement and the individual has requested that the Department include the individual's request for amendment and its denial in subsequent disclosures of PHI, the Department will attach such documents with any subsequent disclosures of PHI.

When a subsequent disclosure is made pursuant to the above using a standard transaction under 45 C.F.R. Part 162 that does not permit the additional material to be included with the disclosure, the Department may separately transmit the material, as required by these procedures, as applicable, to the recipient of the standard transaction.

Documentation of records requested

POLICY 136: Documentation concerning requests for amendments will be maintained in accordance with Policy 352.

Documentation of persons processing access requests

POLICY 138: The Department will document the titles of the persons or offices responsible for receiving and processing requests for amendments by individual and such documentation will be maintained in accordance with Policy 352.

C. Requesting restrictions of uses and disclosures (45 C.F.R. 164.522(a))

General

POLICY 140: The Department will permit individuals to request that the Department restrict uses or disclosures of PHI about the individual to carry out treatment, payment or the Department's operations. DSS must comply with the requested restriction if, the disclosure is to a health plan for the purposes of carrying out payment or health care operations and is not otherwise required by law **and** the PHI 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 the covered entity in full. Note: This will not occur when an individual is on Medicaid because Medicaid providers are not permitted to accept payment from the individual for services that are covered by Medicaid.

Procedures:

Forward all requests for restrictions of uses and disclosures to the Privacy Officer.

Requests for restrictions from the individual or the personal representative must be in writing.

The Privacy Officer will decide if requested restriction is acceptable to the Department. The Department is not required to agree to a restriction.

Limitations to restrictions

a. Emergencies

POLICY 142: If the Department agrees to a restriction, it will not use or disclose PHI in a manner inconsistent with such restriction, except that, if the individual who requested the restriction is in need of emergency treatment and the restricted PHI is needed to provide emergency treatment, the Department may use or disclose the PHI to a health care provider to provide such treatment. If disclosures to a provider occur under these circumstances, the Department must request that the provider not further use or disclose the information. If the Department agrees to a restriction this shall be documented prominently in the individuals records.

b. Other limitations

POLICY 144: Restrictions agreed to by the Department are not effective to prevent the following uses and disclosures:

- Disclosures required by the Secretary of Health and Human Services to

investigate or determine the Department's compliance with the Privacy Rule;
- Uses and disclosures required by law or court order; and
- Disclosures for judicial and administrative proceedings that are initiated by the individual.

Procedures:

If a request for a restriction pertains to one of the above areas, the Privacy Officer will inform the individual, in writing, that the Department cannot agree to the requested restriction. The Privacy Officer will retain, in the individual's record, a copy of the request for a restriction and the notification to the individual of the reason for the denial of the request.

Termination of agreed- upon restriction

POLICY 146: The Department may terminate an agreed-upon restriction if:

- The individual agrees to or requests the termination in writing; or
- The individual orally agrees to the termination and the oral agreement is documented; or
- The Department informs the individual that it is terminating its agreement to a restriction, except that such termination is effective only with respect to PHI created or received after the Department has so informed the individual.

Procedures:

If an individual requests the termination of a restriction or agrees to a termination proposed by the Department, determine whether the termination of the requested restriction is for all PHI maintained by the Department or only for the PHI created or received after the restriction was originally requested.

Document that restriction has been terminated if individual has agreed orally to the termination.

Inform the individual in writing that the restriction has been terminated.

If the Department is terminating its agreement to a restriction, it will document the reason for the termination.

Inform the individual, in writing, that the restriction is no longer in effect with respect to PHI created or received after the restriction has been terminated.

Document that the individual has been informed in writing that the restriction has been removed.

POLICY 148: The Department will document all agreements to, and terminations of, PHI restrictions and retain all information associated with requested restriction in the individual's case record in accordance with Policy 352.

D. Confidential communication requirements (45 CFR 164.522(b))

POLICY 150: The Department will permit individuals to request, and will accommodate reasonable requests by individuals to receive, communications of PHI from the Department by alternative means or at alternative locations, if the individual clearly states that the disclosure of all or part of that information could endanger the individual.

Procedures:

The individual's request to receive communication of PHI by alternative means or locations must be in writing.

The request must clearly state that the disclosure of all or part of the PHI could endanger the individual.

The request must specify the alternative means of disclosure and/ or alternative address or other method of contact requested.

The Department will review each request on a case-by-case basis, to determine whether the request for disclosure by alternative means or at an alternative location is reasonable.

If the Department determines that the individual's request to receive communications of PHI by alternative means or at an alternative location is reasonable and that its failure to accommodate the individual could endanger the individual, the Department will accommodate the request.

If the Department agrees to accommodate the individual's request for alternative means of or alternative location for disclosure, the Department will disclose in accordance with said agreement.

The Department will document, in the individual's record, the alternative method/ means of communication agreed to by the Department.

E. Accounting of disclosures (45 CFR 164.528)

General

POLICY 152: The Department will provide an individual, upon written request, and at no charge, an accounting of certain disclosures of the individual's PHI that it has made during the six years (or shorter, if requested by the individual) prior to the date of the request for an accounting of disclosures. This includes disclosures of PHI made to or by business associates of the Department, of the individual's PHI. The Department is not required to account for disclosures:

- To carry out TPO, i.e., for purposes of administration of the programs;
- To individuals about themselves or to persons involved in the individuals' care in an emergency;
- Pursuant to an authorization from the individual or personal representative;
- Incident to a use or disclosure otherwise permitted or required , provided the minimum necessary requirements have been followed;
- That have been de-identified; and
- That occurred prior to April 14, 2003.

Procedures:

If PHI is disclosed under one of the circumstances above, documentation of the disclosure is not required.

If PHI is disclosed under other circumstances, an accountable disclosure form must be completed and given to the Privacy Officer (CO). Examples of disclosures that must be accounted for are:

- Disclosures required by law that are not for purposes of administration of the Department's programs (e.g., law enforcement, child abuse, elder abuse); and
- Disclosures pursuant to a court order.

Content of the accounting

POLICY 154: The accounting must include, for each disclosure:

- The date of the disclosure;
- The name and, if known, the address of the entity or person who received the disclosure;
- A brief description of the PHI disclosed; and
- 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 copy of the written request for a disclosure from the Secretary of Health and Human Services (if investigating or determining the Department's compliance with the Privacy Rule) or from the requesting entity if the disclosure is required by law.

Provision of the accounting of disclosures

POLICY 156: The Department will act on a request for an accounting no later than 60 days after Receipt of the request by providing the requested accounting. If the Department is unable to provide the accounting within 60 days, the Department may extend the time to provide the accounting by no more than 30 days.

If the accounting is not completed and provided to the individual within 60 days, the Department will inform the individual in writing that the accounting will be provided within an additional 30 days and will state the reasons for the delay and the date by which the Department will provide the accounting.

The Department may have only one such extension of time for action on a request for an accounting.

Procedures:

- Individuals should be told that requests for accountings must be in writing.
- The Privacy Officer will receive the request for accounting.
- The Privacy Officer will check to see whether disclosures for which an accounting must be provided have been made concerning the individual and collect the information necessary to prepare the accounting. The Privacy Officer will check with the region and with the Department's business associates to determine whether disclosures have been made which must be included in an accounting.

- If, during the period covered by the accounting request, multiple disclosures have been made by the Department to the same entity or person for a single purpose under the section of the Privacy Rule requiring disclosures to the Secretary of Health and Human Services to investigate or determine the Department's compliance with the Privacy Rule, or as required by law, the accounting may provide the information required, in Policy 154, for the first disclosure during the accounting period, and then state the frequency, periodicity, or number of the disclosures made during the accounting period and the date of the last such disclosures.

POLICY 158: If a health oversight agency or a law enforcement official provides the Department with a written statement that the provision of an accounting to an individual would be reasonably likely to impede the agency's or official's activities and specifies a time for which the suspension is required, the Department will temporarily suspend an individual's right to receive an accounting of disclosures to said health oversight agency or law enforcement official.

If the agency or official statement is made orally and not in writing, the Department will document the statement; verify the identity of the agency or official making the statement; temporarily suspend the individual's right to an accounting, subject to the statement; and limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement is submitted during that time.

Fees for accountings

POLICY 160: The Department will provide the first accounting to an individual within any 12-month period without charge. For subsequent requests for an accounting by the same individual within the same 12-month period, the Department will inform individuals that it may impose a reasonable, cost-based fee for any subsequent request within the 12- month period and provide him/her with the opportunity to withdraw or modify the request for a subsequent accounting.

Documentation

POLICY 162: The Department documents and maintains, in accordance with Policy 352, the following:

- Written accountings that are provided to individuals;
- The information required to be included in the accounting for disclosures of PHI that are subject to an accounting; and
- Titles of persons or offices responsible for receiving and processing requests for an accounting by individuals.

Section II – Agency Requirements Pertaining to Clients

A. Privacy Notice to Individual Covered By Plans (45 CFR 164.520)

General

POLICY 200: Individuals have the right to adequate notice regarding the uses and disclosures of PHI that may be made by the Department, their rights under HIPAA, and the Department's legal duties with respect to PHI.

Content of Notice of Privacy Practices

POLICY 202: The Department must provide a notice, written in plain language, that includes the following elements:

a. Header:
THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

b. A description, including at least one example, of types of uses and disclosures that the Department is permitted to make for purposes of treatment, payment and health care operations.

c. A description of each of the other purposes for which the Department is allowed or required to use or disclose PHI without the individual's written authorization;

d. If state law or federal Medicaid or other law is more stringent than the Privacy Rule, the descriptions required by (b) and (c) above must reflect the more stringent law, as defined in 45 C.F.R. § 160.202.

e. The descriptors required by (b) and (c) above must include sufficient detail to place the individual on notice of the uses and disclosures that are permitted or required by law.

f. If the Department intends to contact the individual to provide appointment reminders or other health related benefits and services that may be of interest to the individual there must be a separate statement included in the description of uses and disclosures concerning treatment, payment and health care operations ((b) above).

g. A description of the types of uses and disclosures that require an authorization under 45 CFR 164.508(a)(2)-(4), a statement that the Department will make other uses and disclosures only with the individual's written authorization and that the individual may revoke such authorization in writing accordance with 45 CFR 164.508(b)(5) ;

h. A statement of the individual's rights with respect to PHI and a description of how the individual may exercise these rights, as follows:

i. The right to request restrictions on certain uses and disclosures of PHI,

including a statement that the department is not required to agree to a requested restriction, except in the case of a disclosure restricted under 45 CFR 164.522(a)(1)(vi);
ii. The right to receive confidential communications of protected health information, as provided by 45 CFR 164.522(b);
iii. The right to inspect and copy PHI as provided by 45 CFR 164.524;
iv. The right to amend PHI, as provided by 45 CFR 164.526;
v. The right to receive an accounting of disclosures of PHI, as provided by 45 CFR 164.528;
vi. The right to obtain a paper copy of the notice from the Department upon request, even if the individual has agreed to receive the notice electronically;

i. A statement of the Department's duties with respect to PHI, including:

i. the duty to maintain PHI, to provide individuals with notice of its legal duties and privacy practices regarding PHI, and to notify affected individuals following a breach of unsecured protected health information;
ii. the duty to abide by the terms of the notice currently in effect;
iii. the duty to inform the individual that the Department may change the terms of its notice and make the new notice provisions effective for all PHI that it maintains;
iv. the duty to describe how the department will provide individuals with a revised notice;

j. A statement regarding the complaint process, including:

i. a statement that individuals may complain to the Department and to the Secretary of Health and Human Services if they believe their privacy rights have been violated;
ii. a description of how to file a complaint with the Department;
iii. a statement that the Department will not retaliate against an individual for filing a complaint;

k. The name of the Department's contact person, including the name, title and telephone number of a person or office to contact for further information;

l. The effective date of the notice, including the date on which the notice is first in effect, but no earlier than the date on which the notice is printed or otherwise published.

POLICY 204: In order for the Department to apply a change in a privacy practice described in the notice to the PHI the Department created or received prior to issuing a revised notice, the notice must contain a statement that it reserves the right to change the terms of its notice and to make the new notice provisions effective for all PHI that it maintains. This statement must also describe how it will provide individuals with a revised notice.

Revisions to Notice

POLICY 208 : The Department will promptly revise and distribute its notice whenever there is a material change to the uses or disclosures; or the individual's rights; or the Department' legal duties; or other privacy practices stated in the notice. Except when required by law, the Department will not implement said material change prior to the effective date of the notice in which the material change is reflected.

Provision of Notice

POLICY 210: The Department or its Business Associate provides the Notice of Privacy Practices to all individuals who are covered by medical assistance at the time coverage is granted.

POLICY 212: If there is a material change to the notice, the Department posts the revised Notice of Privacy Practices on its website by the effective date of the material change and provides the revised notice in its next annual mailing to individuals who are covered by the medical assistance program.

POLICY 214: At the time of annual redeterminations, the Department notifies individuals of the availability of the Notice of Privacy Practices and how to obtain the notice.

POLICY 216: The Notice of Privacy Practices is provided to the individual in whose name the application for benefits is taken.

POLICY 218: The Department may provide the Notice of Privacy Practices to an individual by email if the individual agrees to electronic notice and such agreement has not been withdrawn. If the Department knows that the email transmission has failed, a paper copy of the notice must be provided to the individual.

POLICY 220: Individuals who receive the Notice of Privacy Practices electronically retain the right to obtain a paper copy of the notice from the Department upon request.

POLICY 222: The Notice of Privacy Practices will be posted prominently at the Department's web site, http://www.ct.gov , and is available for download via the site.

Documentation of compliance

POLICY 224: The Department will retain copies of the Notice of Privacy Practices, in paper or electronic form, in accordance with Policy 352. Also, if the Notice of Privacy Practices is amended, a paper or electronic form of the amended notice shall likewise be kept.

The Privacy Officer keeps a copy of the notice and documentation that the notice was sent to the individuals covered by the Department's medical assistance programs.

B. Minimum Necessary (45 C.F.R. 164.502(b); 45 C.F.R. 164.514(d))

General

POLICY 226: When the Department uses PHI, discloses PHI or requests PHI from another covered entity, the Department makes reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request.

POLICY 228: Minimum necessary **does not** apply to:

- Disclosures to or requests by a health care provider for treatment;

- Permitted uses or disclosures of PHI made to the individual;
- Uses or disclosures made pursuant to an authorization;
- Disclosures made to the Secretary of Health and Human Services; and
- Uses or disclosures that are required by law.
- Uses or disclosures required for compliance with requirements of the HIPAA Privacy and Security Rules

POLICY 230: In the case of disclosure of PHI, the Department determines what constitutes the minimum necessary to accomplish the intended purpose of the disclosure. The Department will not use, disclose, or request an entire medical record, unless the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of such use, disclosure, or request.

Routine and recurring and non-routine and recurring requests by the Department for PHI from other covered entities

POLICY 232: The Department limits all of its requests for PHI to that which is reasonably necessary to accomplish the purpose for which the request is being made, when requesting such information from other covered entities.

Procedures:

Prior to making the request to obtain PHI from another covered entity, consider what PHI is needed and why it is needed.

For non-routine and recurring requests for PHI, review request with Privacy Officer..

For non-routine and recurring requests for PHI, document the request and why it is needed, what type of PHI, and to whom it is going.

Disclosures of PHI to outside individuals or entities

POLICY 234: When the Department discloses PHI on a routine or recurring basis, the use or disclosure is limited to the amount of PHI reasonably necessary to achieve the lawful purpose of the use or disclosure.

Procedures:

Determine if the purpose of the Department disclosure falls into one of the following categories: treatment, payment or operation of the Departments programs.

Determine if the type and amount of information sought is relevant and necessary to accomplish the purpose for which it is sought.

If the purpose of the disclosure falls under the categories of treatment, payment or operations of the Department, release only the minimum amount of PHI necessary to achieve the purpose of the disclosure.

The following steps are to be followed in determining the minimum necessary amount of PHI to accomplish the lawful purpose for which the PHI is sought:

- Identify and analyze the purpose of the disclosures;
- Access only PHI which is directly related to the purpose of the disclosure;
- Identify the individual who is requesting the PHI from the Department and determine if his/her role is directly related to the intended purpose of the disclosure.
- Disclose only that information necessary to accomplish the purpose for which it is disclosed.
- If the purpose is not directly related to treatment, payment, or operations of the Department, do not release the PHI.

If the purpose of the disclosure does not fall under treatment, payment or operations of the Department, do not disclosure PHI unless required by law or with an authorization from the individual.

POLICY 236: The Department reviews all requests for disclosures that are non-routine and non-recurring on an individual basis in accordance with the following criteria:

- Whether the purpose of the disclosure is related to treatment, payment, or operations of a Departmental program;
- Whether the individual making the request needs the PHI in order to assist the Department in the administration of its programs.
- Whether the disclosure is required by law or authorized by the individual.
- Only that PHI which is necessary to accomplish the purpose of the disclosures shall be disclosed.

The Department may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose when (A) Making disclosures to public officials that are permitted, if the public official represents that it is the minimum necessary; (B) the information is requested by another covered entity; or (C) the information is requested by a professional who is a member of its workforce or is a business associate of the covered entity for the purpose of providing professional services to the covered entity, if the professional represents that the information requested is the minimum necessary.

Use of and access to PHI at the Department of Social Services

POLICY 238: The Department will limit use of and access to PHI to that which is reasonably necessary to accomplish the purpose for which access to the PHI is sought.

POLICY 240: The Department identifies classes of persons in its workforce who need access to PHI to carry out their duties and for each such class of person, the categories of PHI to which access is needed.

All members of the Department's workforce are divided in the following table:

Class of Persons	The Department Role Functions	Categories of PHI
Administration	• Managers • Administrators • Contract Administrators	• Medical Information; • Payment Information; • Identifying Information; • Economic Information; • Audit Information; and • Family Information.
Customer Services	• Investigators • Personnel with direct client interaction	• Medical Information; • Payment Information; • Identifying Information; • Economic Information; • Audit Information; and • Family Information.
Administrative Support	• Clerical staff* • Mail Room personnel	• Medical Information; • Payment Information; • Identifying Information; • Economic Information; • Audit Information; and • Family Information.

***Note-** Clerical staff may only access PHI when acting in a customer service capacity.

C. Authorizations for use and disclosure of PHI (45 C.F.R. 164.508)

POLICY 242: The Department may use or disclose PHI (except for psychotherapy notes) for purposes of its own treatment, payment or health care operations (administration of the Department's programs) and may use and disclose all PHI when required by law or court order without obtaining a separate authorization from the individual.

POLICY 244: When disclosure of PHI is <u>not</u> related to the treatment, payment or health care operations (administration of the Department's programs), is psychotherapy notes, or is not required by law or by court order, the Department must obtain the individual's written authorization prior to disclosure of information. Upon receipt of a valid authorization from the individual, the Department will use or disclose PHI consistent with the terms of the authorization form.

Authorizations would also be required if the Department wanted to use an individual's PHI for marketing or if the Department were to sell an individual's PHI. The Department, however, does not use individuals' PHI for such purposes.

If the Department were to directly or indirectly receive remuneration in exchange for any PHI of an individual, or use an individual's PHI for marketing purposes, it must obtain from the individual a valid authorization in accordance with 45 C.F.R. 164.508. The authorization would need to state that the disclosure was being used for marketing purposes or is

being exchanged for remuneration to the Department.

Procedures for obtaining authorizations:

Responses to legislators, advocates and attorneys about individual clients generally do not fall under the category of treatment, payment or any of the Departments operations and require an authorization from the client.

When a legislator, advocate or attorney (or other similar category of persons) calls the Department requesting information about a particular client, thank the person for his or her concern for the individual and explain that the information being sought is PHI. Inform him/her that we need an authorization from the individual in order to release the requested information.

Alternatives:

- Provide authorization form to requesting party and indicate that it must be completed by the individual and returned to the Department.

- Offer to contact the individual and inform the individual that a legislator, advocate or attorney has contacted the Department on his or her behalf and the Department requests authorization to discuss the case with the representative.

The Department may email, , mail or fax an authorization form (or the requesting party may do the same if he or she has forms) to the individual. Do not disclose information to the requesting party until the authorization form comes back to the Department, signed.

- Offer to communicate directly with the individual to attempt to solve the individual's problem
- Respond to the requestor generally, citing rules that apply generally to the issue and explaining the Department's policies concerning the issue.

Note: If it can be established that the legislator, advocate or attorney is involved with the individual's health care or payment related to the individual's health care and is seeking PHI directly relevant to such person's involvement, the Department 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 PHI that is directly relevant to the person's involvement with the individual's care or payment related to the individual's health care. The Department may use professional judgment and its 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.

POLICY 246: For disclosure of psychotherapy notes, the Department must obtain an authorization for their use or disclosure, <u>except</u>:

- as required by the Secretary of Health and Human Services to investigate or determine the Department's compliance with the Privacy Rule;
- as required by law or court order;
- to investigate fraud or abuse of a Department program by the originator of the psychotherapy notes;
- as necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public and is to a person reasonably able to prevent or lessen the threat, including the target of the threat; and
- to carry out the following treatment, payment or health care operations:
    - ♦ Use by the originator of the psychotherapy notes for treatment;
    - ♦ Use or disclosure by the Department for its own training programs in which students, trainees, or practitioners in mental health learn under supervision to

practice or improve their skills in group, joint, family, or individual counseling; or
♦ Use or disclosure by the Department to defend itself in a legal action or other legal proceeding brought by the individual.

POLICY 248: An authorization for use or disclosure of PHI may not be combined with any other document, except as follows:

- An authorization for the use or disclosure of PHI for a research study may be combined with any other type of written permission for the same research study, including another authorization for the use or disclosure of PHI for such research or a consent to participate in such research;
- An authorization for use or disclosure of psychotherapy notes may be combined with another authorization for a use or disclosure of psychotherapy notes, but not with an authorization for the use and disclosure of other PHI;
- An authorization for the use or disclosure of PHI (not psychotherapy notes) may be combined with another authorization for use and disclosure of PHI (not psychotherapy notes).

POLICY 250: An individual may revoke an authorization at any time, provided that the revocation is in writing, except to the extent that the Department has already taken action in reliance on the authorization.

POLICY 252: A valid authorization must contain the following elements:

• A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;

• The name or other specific identification of the person or class of persons at the Department who is authorized to make the requested use or disclosure;

• The name or other specific identification of the person or class of persons to whom the Department is authorized to make the disclosure;

• 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.

• 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 PHI for research, including the creation and maintenance of a research database or repository.

• The signature of the individual and date. If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual must be provided.

POLICY 254: A valid authorization shall also contain statements adequate to place the individual on notice of all of the following:

- The individual's right to revoke the authorization and that the revocation must be in writing to the Department, except if the Department has already taken action in reliance on the authorization.
- The Department may not condition payment, enrollment or eligibility for benefits on the provision of an authorization.
- The potential for information disclosed pursuant to an authorization to be subject to redisclosure by the recipient and no longer protected by the Privacy Rule.

POLICY 256: The Department's authorization form must be written in plain language.

POLICY 258: If the Department seeks and obtains an authorization from an individual for a use or disclosure of PHI, the Department must provide the individual with a copy of the signed authorization.

POLICY 260 An authorization is not valid if it has any of the following defects:

- The expiration date has passed or the expiration date is known by the Department to have occurred;
- The authorization has not been filled out completely with respect to any of the required elements described herein;
- The authorization is known by the Department to have been revoked;
- The authorization is an impermissible compound authorization or conditions the provision of treatment, payment, enrollment in the health plan or eligibility for benefits on the provision of an authorization.
- Any material information in the authorization is known by the Department to be false.

D. Verification of identification and authority requirements (45 CFR 164.514(h).

For all disclosures of PHI

POLICY 262: Prior to any disclosure of PHI by the Department, the Department verifies the identity of the person or entity requesting the PHI and the authority of such person or entity to have access to the PHI, if the identity or authority is not known to the Department.

Procedures

If a requester's identity is known to the Department, either by its agency name, telephone number, fax number, or based on knowledge of a person's voice and/or appearance, there is no need to further verify that person or entity's identity or authority.

If Department staff has reason to question the identity of the person requesting PHI and the

request is being made in person, the staff will further verify the person's identity by requesting to see identification in the form of a license, other picture identification, a business card, or any other reliable form of identification.

If Department staff has reason to question the identity of the person requesting PHI and the request for PHI is being made by telephone, Department staff will find out the caller's affiliation and then verify that the telephone number provided by the requestor is that of the organization or agency the requestor represents. Department staff will ask for the client's identification number and social security number for verification purposes.

If Department staff has reason to question the authority of the person requesting the PHI to obtain the PHI, the Department will require that the requestor either produce the written document that allows him or her to have access to the PHI; or cite to the statute or regulation that entitles the requester to have the information.

If either oral or written documentation, statements, or representations are necessary as a condition of disclosure, said documentation, statements or representations will be presented to Department staff.

For disclosures of PHI to Public Officials

POLICY 264: For disclosures of PHI to a public official or those acting on behalf of a public official, the Department may rely, if such reliance is reasonable under the circumstances, on any of the following to verify the identity of the public official or representative of the public official:

- Presentation of an agency identification badge, other official credentials, or other proof of government status, if the request is made in person;
- The request is made on the appropriate government letterhead, if the request is made in writing;
- If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract, memorandum of understanding, or purchase order that establishes that the person is acting on behalf of the public official.

Procedures:

Upon receiving an in-person request for disclosure of PHI from a public official or representative of a public official, the Department requests that the person present identification to verify his or her identity.

The Department staff makes a copy of the identification and place it in the individual's record or documents in the record that verification of identity was obtained.

If the request for disclosure of PHI is made in writing, it must be on appropriate government letterhead and the request will be placed in the individual's record.

If the person requesting the PHI is a person acting on behalf of a public official, the Department requests that the person submit a written statement of his or her governmental authority to act on behalf of the governmental official.

POLICY 266: For disclosures of PHI to a public official or a person acting on behalf of a public official, the Department may rely, if such reliance is reasonable under the circumstances, on any of the following to verify the authority of the public official or representative of the public official:

1. A written statement citing the legal authority pursuant to which the information is requested; and
2. If the request is pursuant to legal process, a copy of the court order or a subpoena will be presumed to constitute verification of legal authority.

Procedures

Upon receiving a request for PHI, Department staff request a written statement from the public official or representative of the public official indicating his or her legal authority to request the information. If the individual has executed an authorization to allow the Department to release PHI to the government official or a person acting on behalf of the public official, said authorization will constitute the requisite legal authority.

A copy of said statement of legal authority or the authorization is placed in the individual's record.

If the request is made pursuant to a subpoena or court order, a copy of the document is placed in the individual's record.

E. Uses and disclosures of PHI (45 CFR 164.502)

For purposes directly related to administration of the Department's programs

POLICY 268: The Department releases the minimum necessary information concerning the individual for purposes directly connected with the administration of its programs. These purposes include, but are not limited to:

a. Establishing eligibility for and determining amount of assistance;
b. Providing services under the programs
c. Investigating or prosecuting individuals related to the administration of the program, including civil or criminal proceedings. In this context, "related to administration of the program" includes collecting overpayments or other recoveries; investigating fraud cases; locating legally liable relative, when required by law; and auditing or similar activity in connection with the operation of the program by any governmental entity authorized by law to conduct such audit or activity
d. Verification of income obtained under the Income Verification Eligibility System (IVES)
e. FOR Temporary Family Assistance (TFA) AND Supplemental Nutrition Assistance Program (SNAP), this also includes the administration of other federal or federally assisted program which provides assistance in cash, or in kind, or services directly to individuals on the basis of need and certification of the receipt of TFA to an employer for purposes of claiming tax credit under Public Law 94-12, the Tax Reduction Act of 1975.

Use and disclosures of information for administration of the SNAP (7 CFR 272.1)

Use or disclosure of information obtained from SNAP applicant or recipient households shall be restricted to:

1. Persons directly connected with the administration or enforcement of the provisions of the Food Stamp Act or regulations, other Federal assistance programs, federally-assisted State programs

providing assistance on a means-tested basis to low income individuals, or general assistance programs which are subject to the joint processing requirements.

2. Persons directly connected with the administration or enforcement of the programs which are required to participate in the State income and eligibility verification system (IEVS) as specified in § 272.8(a)(2), to the extent the SNAP information is useful in establishing or verifying eligibility or benefit amounts under those programs;
3. Persons directly connected with the verification of immigration status of aliens applying for SNAP benefits, through the Systematic Alien Verification for Entitlements (SAVE) Program, to the extent the information is necessary to identify the individual for verification purposes.
4. Persons directly connected with the administration of the Child Support Program under part D, title IV of the Social Security Act in order to assist in the administration of that program, and employees of the Secretary of Health and Human Services as necessary to assist in establishing or verifying eligibility or benefits under titles II and XVI of the Social Security Act;
5. Employees of the Comptroller General's Office of the United States for audit examination authorized by any other provision of law; and
6. Local, State, or Federal law enforcement officials, upon their written request, for the purpose of investigating an alleged violation of the Food Stamp Act or regulation. The written request shall include the identity of the individual requesting the information and his authority to do so, violation being investigated, and the identity of the person on whom the information is requested.
7. Local, State or Federal law enforcement officers, upon written request, for the purpose of obtaining the address, social security number, and, if available, photograph of any household member,
   a. if the member is fleeing to avoid prosecution or custody for a crime, or an attempt to commit a crime, that would be classified as a felony, or is violating a condition of probation or parole imposed under a Federal or State law.
   b. upon the written request of a law enforcement officer acting in his or her official capacity, where such member has information necessary for the apprehension or investigation of another member who is fleeing to avoid prosecution or custody for a felony, or has violated a condition of probation or parole.
   c. to the extent that the Department discloses only such information as is necessary to comply with a specific written request of a law enforcement agency authorized by this paragraph.
8. Local educational agencies administering the National School Lunch Program for the purpose of directly certifying the eligibility of school-aged children for receipt of free meals under the School Lunch and School Breakfast programs based on their receipt of SNAP.

For purposes required by law but not for administration of the Department's programs

POLICY 270: The Department releases the minimum necessary information concerning individuals as required by law. If staff is in doubt about whether **a** disclosure should be made, staff should consult with the Privacy Officer, or a Department attorney. All disclosures under this Part shall be documented in individuals' records.

a. Law Enforcement Officers: For all Department programs except the Medicaid program, the Department will disclose to a federal, state or local law enforcement officer, upon the officer's request, the current address of any recipient if the officer

i. furnishes the Department with the name of the individual;

ii. notifies the Department that the location or apprehension of the individual is within the officer's official duties; and

iii. notifies the Department that the individual

(A) is fleeing to avoid prosecution, custody or confinement after conviction, under the laws of the place from which the individual is fleeing, for a crime, or an attempt to commit a crime, which is a felony under the laws of the place from which the individual is fleeing, or, in the case of the State of New Jersey, is a high misdemeanor under the laws of that state; or

(B) is violating a condition of probation or parole imposed under federal or

state law; or
(C) has information that is necessary for the officer to conduct the official duties of that office.

b. The Department of Children and Families ("DCF"):
i. For all Department programs, upon a request from DCF, the Department will disclose to DCF necessary information concerning a child or the immediate family of a child who receives the Department's benefits if the child's health, safety or welfare is in imminent danger, as determined by DCF, and the disclosure is to only the Commissioner of DCF or an official designee.
ii. For all Department programs, if the Department has reason to believe that any child under the age of 18 is being subjected to physical or mental abuse or neglect while in the care of a parent or other person responsible for the child's care, the Department will notify the Commissioner of DCF or an official designee.

Procedure

Once it is determined that disclosure to DCF is required by law, the Department discloses as appropriate and documents in the individual's case record that disclosure to DCF has been made.

If the Department releases PHI in its disclosure to DCF, the Department staff notifies the Privacy Officer for purposes of the accounting.

c. Office of the Child Advocate

For all Department programs, except Medicaid and SNAP, the Department will disclose to the Child Advocate any records necessary to carry out the responsibilities of the Child Advocate as provided in subsection (a) of section 46a-13l of the Connecticut General Statutes. If the Child Advocate is denied access to any records necessary to carry out said responsibilities, the Child Advocate may issue a subpoena for the production of such records.

d. Disclosures to Other Government Agencies

The Department discloses PHI about individuals where uses and disclosures are required by law, as follows:

i. For all Department programs, except the Medicaid and SNAP, to any authorized representative of the Labor Commissioner such information directly related to unemployment compensation administered pursuant to chapter 567 of the Connecticut General Statutes or information necessary for implementation of sections 17b-688b to 17b-688d, inclusive, and section 122 of public act 97-2 of the June 18 special sessions: ;

ii. For all Department programs, except SNAP, to the Commissioner of Mental Health and Addiction Services any information necessary for the implementation and operation of the basic needs supplement program or the Medicaid program for low-income adults, established pursuant to section 17b-261n;

iii. To the Commissioner of Administrative Services and the Commissioner of Emergency Services and Public Protection, such information as the Commissioner of Social Services determines is directly related to and necessary for these agencies for purposes of performing their functions of collecting social services recoveries and overpayments and amounts due as support in social services cases,

investigating social services fraud or locating absent parents of public assistance recipients;

iv. To any town official or other contractor or authorized representative of the Labor Commissioner such information concerning an applicant or recipient of assistance under state-administered general assistance deemed necessary by said the Commissioners of Social Services and the Labor Commissioner to carry out their respective responsibilities to serve such persons under the programs administered by the Labor Department that are designed to service applicants for and recipients of State-Administered General Assistance (SAGA);

v. For all Department programs, except the Medicaid and SNAP, to any authorized representative of the Department of Public Health or the Office of Early Childhood to carry out his or her respective responsibilities under the programs that regulate child day care services or youth camps.

vi. To the Department of Public Health to coordinate operation of the Medicaid program with:

(A) the state's operation of the Special Supplemental Food Program for Women, Infants and Children ("WIC");

(B) programs funded under Title V;

(C) the Department of Public Health's survey functions for the purpose of maintaining health standards for institutions that provide services to Medicaid recipients.

vii. For all Department programs, except the Medicaid program, to the Department of Correction, in IV-D support cases, information concerning noncustodial parents that is necessary to identify inmates or parolees with IV-D support cases who may benefit from Department of Correction educational, training, skill building, work or rehabilitation programming that will significantly increase an inmate's or parolee's ability to fulfill such inmate's support obligation;

viii. For all Department programs, except Medicaid, to the Judicial Branch, in IV-D support cases, information concerning non-custodial parents that is necessary to (A) Identify non-custodial parents with IV-D support cases who may benefit from educational, training, skill building, work or rehabilitation programming that will significantly increase such parent's ability to fulfill such parent's support obligations, (B) assist in the administration of the Title IV-D child support program, or (C) assist in the identification of cases involving family violence;

ix. To the State Treasurer in IV-D support cases, information that is necessary to identify child support obligors who owe overdue child support prior to the Treasurer's payment of such obligor's claim for any property unclaimed or presumed abandoned under part III of chapter 32.

x. To any authorized representative of the Commissioner of Housing for the purpose of verifying whether an applicant for the renters rebate program established by section 12-170d, as amended by this act, is a recipient of cash assistance from the Department of Social Services and the amount of such assistance (SAGA clients only).

e. IV-D support cases

For all Department programs, except Medicaid and SNAP, to a health insurance provider, in IV-D support cases, information concerning a child and the custodial parent of such child that is necessary to enroll such child in a health insurance plan available through such provider when the noncustodial parent of such child is under court order to provide health insurance coverage but is unable to provide such information, provided the Commissioner of Social Services determines, after providing prior notice of the disclosure to such custodial parent and an opportunity for such parent to object, that such disclosure is in the best interests of the child.

Responding to subpoenas

POLICY 272 : The Department accepts service of subpoenas and complies with them only upon the issuance of a court order after having informed the court of the applicable state and federal statutory provisions, policies and regulations restricting disclosure of information.

Procedure:

If a subpoena is issued to a specific employee of the Department (other than the Commissioner or Deputy Commissioners), only that employee should accept service of the subpoena. If that employee is not in the office at the moment or on vacation, the marshal will need to return to the office to serve that employee.

Employees should accept services of subpoenas that are addressed to the keeper of the records or the custodian of the records.

Upon being served with a subpoena, staff should fax or email the subpoena to the Department's Office of Legal Counsel.

Responding to discovery requests

POLICY 274: In the event that the Department cannot redact PHI from a Department record, the Department will obtain a qualified protective order from the court or, as agreed to by the parties, prior to the release of documents that contain PHI.

Procedure:

Upon receipt of a discovery request, the request will be forwarded to the Department's Office of Legal Counsel or the Attorney General's Office.

Disclosures of the PHI of deceased individuals

POLICY 276: The Department complies with the HIPAA privacy rule with respect to the PHI (other than confidential HIV-related information, psychiatric and substance abuse information) of a deceased individual for a period of 50 years following the death of the individual.

Disclosures to personal representatives

POLICY 278 : Except as otherwise required by law or if it is not in the best interest of the individual, the Department will treat a personal representative as the individual for purposes of disclosure of PHI.

a. Adults and Emancipated Minors: If a person has the authority to act on behalf of an individual who is an adult or an emancipated minor in making health care decisions, the Department will treat such person as a personal representative for purposes of disclosure of PHI.

b. Unemancipated Minors: If a parent, guardian, or other person *acting in loco parentis* has the authority to act on behalf of an individual who is an unemancipated minor in making health care decisions, the Department will treat such person as the personal representative with respect to disclosure of PHI, except if:

i. the minor consents to the health care service; no other consent is required by 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;

ii. the minor may lawfully obtain a particular health care service without the consent of the 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;

iii. a parent, guardian or other person acting *in loco parentis* assents to an agreement of confidentiality between a covered health care provider and the minor with respect to such health care service.

iv. the parent, guardian or other person acting *in loco parentis* seeking information about the individual is not the personal representative of the individual. In that case, the decision whether to give access to the parent, guardian or person acting in loco parentis must be made by a licensed health care professional in the exercise of professional judgment and be consistent with applicable law.

c. Deceased Individuals: If the executor, administrator, or other person has authority to act on behalf of a deceased individual, or on behalf of the individual's estate, the Department must treat that person as a personal representative with regard to PHI that is relevant to the representation.

d. Abuse, Neglect, Endangerment Situations: The Department may choose not to treat a person as the personal representative if the Department has reason to believe that the individual has been or may be subjected to domestic violence, abuse or neglect by such person; or treating such person as the personal representative could endanger the individual and the Department, 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.

Disclosures to persons involved with health care or payment for health care for the individual

POLICY 280: When the individual is present and available, i.e., has the capacity to make health care decisions, the Department may disclose to a family member, relative or a close friend of the individual or any other person identified by the individual PHI that is directly relevant to such person's involvement with the individual's care or payment for the health care if the individual agrees, does not object, or the Department can reasonably infer from the circumstances, based on professional judgment, that the individual does not object to the disclosure.

POLICY 282: When the individual is not present or does not have the opportunity to agree to the use or

disclosure of PHI because of the individual's incapacity or an emergency circumstance, the Department may, in the exercise of professional judgment, disclose to another person only that PHI which is directly relevant to the person's involvement with the individual's care. The Department may use professional judgment and its 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 obtain the individual's PHI.

POLICY 283: If the individual is deceased, the Department may disclose to a family member, other relative, a close personal friend of the individual or any other person identified by the individual who were involved in the individual's care or payment for health care prior to the individual's death, PHI (except confidential HIV-related information, psychiatric and substance abuse information) of the individual that is relevant to such person's involvement, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the Department.

F. Prohibition Against Retaliation (45 CFR 164.530(g))

POLICY 284: The Department does not intimidate, threaten, coerce, discriminate against, or take any other retaliatory action against any individual who is exercising his or her rights, or is participating in, any process established by the Privacy Rule or the Breach Notification Rule, including the filing a complaint against the Department or the Secretary of Health and Human Services alleging its failure to follow these rules.

POLICY 286: The Department does not require individuals to waive their rights to make a complaint to the Secretary of Health and Human Services or any of their rights under the Privacy Rule or the Breach Notification Rule as a condition of obtaining services from the Department.

G. De-identification of information (45 CFR 164.514)

POLICY 288: The Department de-identifies PHI of individuals that is sought by other entities, unless the other entities are the Department's business associates; are using the PHI for purposes of administration of the Department's programs; or present the Department with HIPAA-compliant authorizations signed by the individuals or their personal representatives. 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 would be considered de-identified.

Procedures

The Department determines the method of de-identification on a case-by-case basis. A person at the Department with appropriate knowledge of, and experience with, generally accepted statistical and scientific principles and methods for rendering information not individually identifiable, may determine 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 the subject of the information and document the methods and results of the analysis that justify the determination;

or

The Department removes the identifiers of the individual or of relatives, employers, or household members of the individual, by removing the following:

a. Names;
b. All geographic subdivisions smaller than a State, including street address, 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:

1. The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; ***and***
2. The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

c. 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;
d. Telephone numbers;
e. Fax numbers;
f. Electronic mail addresses;
g. Social security numbers;
h. Medical record numbers;
i. Health plan beneficiary numbers;
j. Account numbers;
k. Certificate/ license numbers;
l. Vehicle identifiers and serial numbers;
m. Device identifiers and serial numbers;
n. Web Universal Resource Locators (URLs);
o. Internet Protocol (IP) address numbers;
p. Bio-metric identifiers, including finger and voice prints;
q. Full face photographic images and any comparable images;
r. Any other unique identifying number, characteristic, or code, except as permitted; and
s. The department 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.

POLICY 290: The Department may assign a code or other means of record identification to allow de-identified records to be re-identified, provided that the code or other means of record identification is not derived from, or related to, information about the individual and is not otherwise capable of being translated so as to identify the individual and the Department does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification.

H. Limited data set and Data use agreement (45 C.F.R. 164.514(e))

POLICY 291: The Department may disclose a limited data set that meets the requirements in Policy 292 if the Department enters into a data use agreement with the limited data set recipient that meets the requirements in Policy 296.

POLICY 292: A limited data set is PHI that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:

a. Names;
b. Postal address information, other than town or city, State, and zip code;
c. Telephone numbers;

d. Fax numbers;
e. Electronic mail addresses;
f. Social security numbers;
g. Medical record numbers;
h. Health plan beneficiary numbers;
i. Account numbers;
j. Certificate/ license numbers;
k. Vehicle identifiers and serial numbers; including license plate numbers;
l. Device identifiers and serial numbers;
m. Web Universal Resource Locators (URLs);
n. Internet Protocol (IP) address numbers;
o. Bio-metric identifiers, including finger and voice prints; and
p. Full face photographic images and any comparable images.

Procedures

Requests from entities to enter into limited data sets with the Department shall be forwarded to and discussed with the DSS Privacy Officer.

The Department shall have a template for a data use agreement for use as determined by the DSS Privacy Officer and legal counsel.

POLICY 293: The Department may use or disclose a limited data set only for the purposes of research, public health, or health care operations.

POLICY 294: The Department may use PHI to create a limited data set or disclose PHI only to a business associate so that the business associate may create the limited data set for such purpose, whether or not the limited data set is to be used by the Department.

POLICY 295: The Department may use or disclose a limited data set only if the

Department obtains satisfactory assurance, in the form of a data use agreement that meets the requirements set forth below, that the recipient of the limited data set will use or disclose the PHI (in the form of a limited data set) only for limited purposes.

POLICY 296: The data use agreement between the Department and the limited data set recipient must meet the requirements of 45 C.F.R. § 164.514(e)(4) in that it must:

• Establish the permitted uses and disclosures of such information by the limited data set recipient, consistent with policies 293 and 294. The data use agreement may not authorize the limited data set recipient to use or further disclose the information in a manner that would violate the requirements of Subpart E of 45 C.F.R. Part 164 (Privacy of Individually Identifiable Health Information), if done by the Department.
• Establish who is permitted to use or receive the limited data set; and
• Provide that the limited data set recipient will:
  • Not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law;
  • Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement;
  • Report to the Department any use or disclosure of the information not provided for by its data use agreement of which it becomes aware;
  • Ensure that any agents, including a subcontractor to whom it provides the limited

data set agrees to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and
• Not identify the information or contact the individuals.

POLICY 297: The Department is not in compliance with the requirements set forth above and contained in 45 C.F.R. § 164.514(e) if the Department knew of a pattern of activity or practice of the limited data set recipient that constituted a material breach or violation of the data use agreement, unless the Department took reasonable steps to cure the breach or end the violation, as applicable. If the steps taken by the Department are unsuccessful, the Department must discontinue disclosure of PHI (in a limited data set) to the recipient and report the problem to the Secretary of Health and Human Services.

POLICY 298: If the Department is a limited data set recipient and violates a data use agreement, the Department will be in noncompliance with the requirements set forth above and contained in 45 C.F.R. § 164.514(e).

Section III: Agency Operational Requirements

A. Personnel designations (45 CFR 154.530)

POLICY 300: The Department designates a privacy official in Central Office who is responsible for the development and implementation of the policies and procedures of the Department regarding the Privacy Rule; is the contact person responsible for receiving complaints concerning noncompliance with the Privacy Rule; and provides further information about the Notice of Privacy Practices.

B. Training (45 CFR 164.530)

POLICY 304: The Department provides training to all members of the workforce on the policies and procedures developed by the Department to implement the Privacy Rule (Subpart E) and the breach notification requirements (Subpart D), as necessary and appropriate for staff to carry out their functions within the Department :

• Upon employment, Department staff must take an online HIPAA training.
• When there are new requirements or changes in HIPAA policies and procedures, the training is updated and staff is informed of the changes.
• All staff must take an annual refresher training that addresses the HIPAA Privacy and Security Rules and breach notification requirements.

POLICY 306: In the event of a material change in the Department's policies and procedures required by the HIPAA regulations, the Department trains staff whose functions are affected by the material change. Such training will occur either before or within a reasonable period of time after the material change becomes effective.

POLICY 308: The Department documents that training has been provided and retain in accordance with Policy 352, the following:

• Training materials;
• Final training plans;

• Attendance rosters; and
• Skills evaluations pertaining to Privacy Rule policies and procedures training.

C. Business associates and business associate contracts (45 CFR 164.502, 164.504)

General

POLICY 310: The Department may disclose PHI to a business associate and may permit the business associate to create, receive maintain or transmit PHI on the Department's behalf as long as the Department obtains satisfactory assurances that the business associate will appropriately safeguards the PHI. The Department is not required to obtain such satisfactory assurances from a business associate that is a subcontractor, i.e., a business associate's contractor.

For those Department contractors that are "business associates," as the term is defined in 45 C.F.R. § 160.103, the Department's contracts contain business associate agreements, as required by the Privacy Rule.

Healthcare providers to whom or which the Department discloses information for purposes of treatment of the individual are not considered business associates. (See definition section of this manual or 45 CFR 160.103)

POLICY 312: Business associate agreement must meet the requirements of 45 C.F.R. § 164.504(e)(2).

The business associate agreement:

- establishes the permitted and required uses and disclosures of PHI by the business associate.

- may not authorize the business associate to use or further disclose the information in a manner that would violate the requirements of the Privacy Rule, if done by the Department, except that it may permit the business associate to use and disclose PHI for the proper management and administration of the business associate, as it pertains to the Department, and to carry out its legal responsibilities, as they pertain to the Department, only if disclosure is required by law or the business associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or disclosed only as required by law or for the purpose for which it was disclosed to the person and the person notifies the business associate of any instances of which it is aware in which the confidentiality of the information has been breached.

- may permit the business associate to provide data aggregation services related to the health care operations of the Department.

- authorizes termination of the contract by the Department if the Department determines that the business associate has violated a material term of the contract.

- provide that the business associate must:

  • not use or further disclose information other than as permitted or required by the contract or as required by law;

  • use appropriate safeguards and comply, where applicable, with the security standards for protection of electronic PHI with respect to electronic PHI, to prevent use or disclosure of the information other than as provided for by the contract;

• report to the Department any use or disclosure of the information not provided for by its contract of which it becomes aware, including breaches of unsecured protected health information, as required by the breach notification rules;

• ensure that any subcontractors that create, receive, maintain or transmit PHI on behalf of the business associate agree to the same restrictions and conditions that apply to the business associate with respect to such information;

• make available PHI in accordance with section 164.524 (access of individuals to PHI);

• make available PHI for amendment and incorporate any amendments to PHI in accordance with section 164.526 (amendment of PHI);

• make available the information required to provide an accounting of disclosures in accordance with 164.528 (accounting of disclosures of PHI);

• to the extent the business associate is to carry out the Department's obligation under the Privacy Rule, comply with the requirements of the Privacy Rule that apply to the Department in performance of its obligations;

• make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by, the business associate on behalf of the Department available to the Secretary of Health and Human Services for purposes of determining the Department's compliance with the Privacy Rule;

• at termination of the contract, if feasible, return or destroy all PHI received from, or created or received by the business associate/contractor on behalf of the Department that the business associate still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible;

POLICY 314: If a business associate of the Department is another governmental entity, then the Department may enter into a memorandum of understanding with the business associate that contains terms that accomplish the objectives of 45 C.F.R. 164.504(e)(2), as set forth above, and 45 C.F.R. 164.314(a)(1), if applicable.

If a business associate that is a governmental entity is required by law to perform a function or activity on behalf of the Department or to provide services to the Department described in the definition of *business associate* in section 160.103 of the Privacy Rule, then the Department may disclose PHI to the contractor to the extent necessary to comply with the legal mandate without meeting the business associate requirements of 164.504(e) and 164.314(a), provided that the Department attempts in good faith to obtain satisfactory assurances by entering into a memorandum of understanding with the business associate that accomplishes the objectives of 45 C.F.R. §164.504(e)(2) and 164.314(a). If such attempt fails, the Department documents the attempt and the reasons such assurances cannot be obtained.

If authorization for termination is inconsistent with the statutory obligations of the Department or its business associate, the Department may omit the termination authorization required by 164.504(e)(2)(iii).

The Department may comply with 45 C.F.R. 164.504(e) and 45 C.F.R. 164.314(a)(1) if it

discloses only a limited data set to a business associate for the business associate to carry out a health care operations function and the covered entity has a data use agreement with the business associate that complies with 45 C.F.R. 164.514(e)(4) and 164.314(a)(1), if applicable.

POLICY 316: The Department is not in compliance with the business associate provisions of the Privacy Rule if it knew of a pattern of activity or practice of a business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the Department took reasonable steps to cure the breach or end the violation, as applicable, and if such steps were unsuccessful, terminated the contract or arrangement, if feasible.

POLICY 320: The Department will document the satisfactory assurances it receives from its business associates indicating that the business associates will appropriately safeguard the information it obtains from the Department through a written contract, memorandum of understanding or other document that meets the requirements of section 164.502(e)(2) of the Privacy Rule.

Effect of Prior Contracts or other Arrangements with Business Associates (45 CFR 164.532(e))

POLICY 322: If, prior to January 25, 2013, the Department entered into and is operating pursuant to written contracts and business associate agreements that complied with the law in effect at that time and such contracts are not renewed or modified from March 26, 2013 until September 23, 2013, then the Department is deemed to be in compliance with the requirements pertaining to business associate agreements until the earlier of (i) the date such contract or other arrangement is renewed or modified on or after September 23, 2013 or (ii) September 22, 2014.

POLICY 324 : Notwithstanding the above, the Department is required to comply with Subpart C of 45 C.F.R. Part 160 and the provisions of the Privacy Rule pertaining to amendment of PHI, access to PHI, accounting, and mitigation with respect to PHI held by a business associate.

D. Complaints to the Department and Secretary of Health and Human Services (45 CFR 164.530(d))

Complaints to the Department

POLICY 326: The Department provides a process for individuals to make complaints concerning the Departments policies and procedures required by the Privacy Rule and the Breach Notification Rule or its compliance with such policies and procedures or requirements.

Procedures:

If an individual wishes to make a complaint concerning the Department's compliance with the Privacy Rule of the Breach Notification Rule, the client is given the name, telephone number and email address of the Privacy Officer.

Upon receipt of a verbal complaint, the Privacy Officer will document the complaint. All written complaints will be forwarded to the Privacy Officer. The Privacy Officer will address the individual's complaint and document all actions taken in response to it in accordance with Policy 352.

Complaints to the Secretary of Health and Human Services

POLICY 328 : The Department provides a process for individuals to make complaints to the Secretary of Health and Human Services concerning the Departments policies and procedures required by the Privacy Rule and the Breach Notification Rule or its compliance with such policies, procedures or requirements.

Procedures:

If an individual wishes to make a complaint concerning the Department's compliance with the Privacy Rule or the Breach Notification Rule, the Privacy Office gives the individual the necessary contact information and requirements for filing a complaint to the Office for Civil Rights within the Department of Health and Human Services.

E. Mitigation of any harmful effect known to a use or disclosure of protected health information (45 CFR 164.530(f))

POLICY 330: The Department mitigates, to the extent practicable, any harmful effects that it knows about, of a use or disclosure of PHI in violation of any of the Department's HIPAA policies or procedures, or the requirements of the Privacy Rule, by the Department or any of its business associates.

Procedures:

If a member of the Department's workforce becomes aware of any harmful effect of a use or disclosure in violation of the Privacy Rule, such use or disclosure must be reported immediately to the Privacy Officer..

The Privacy Officer will take whatever steps are reasonable to address and mitigate an improper disclosure.

F. Sanctions (45 CFR 164.530(e))

POLICY 332: The Department has and applies appropriate sanctions against members of its workforce who fail to comply with the Department's policies and procedures required by the Privacy Rule and the Breach Notification Rule. This standard does not apply to a member of the workforce with respect to actions covered by and that meet the conditions of Policy 334 and Policies 284 and 286

When considering the level of sanction to apply, the Department consult state and federal law, in addition to union contracts, and any other relevant personnel policies. The Department will document the sanctions it applies, if any, and retain said documentation in accordance with Policy 352.

G. Disclosures by whistleblowers (45 CFR 164.502(j))

POLICY 334: The Department is not in violation of Privacy Rule if a member of its workforce or a business associate discloses PHI for the purpose of making a whistleblower complaint, provided that:

• The workforce member or business associate believes in good faith that the Department has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the Department potentially

endangers one or more clients, workers, or the public; and
• The disclosure is made in compliance with section 4-61dd of the Connecticut General Statutes or to a health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the Department.

POLICY 336: In making a whistleblower complaint, an employee will release only that PHI which is minimally necessary for the complaint to be acted upon by the Auditors of Public Accounts in accordance with section 4-61dd of the Connecticut General Statutes, or to such other oversight agency, as appropriate.

H. Safeguards (45 CFR 164.530((a)(2))

POLICY 338: The Department has in place appropriate administrative, technical, and physical safeguards to protect the privacy of individuals' PHI.

POLICY 340: The Department reasonably safeguards PHI to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.

POLICY 342: The Department reasonably safeguards PHI from any intentional or unintentional use or disclosure that is in violation of the requirements of the Privacy Rule.

Procedures:

The Department educates all employees with access to PHI on the confidentiality of health information.

The Department controls access to and protect the physical security of PHI from loss, damage, destruction, acts of mischief and casual observation by storing and maintaining PHI in secure locations.

Individuals with access to PHI are responsible to protect the information from unauthorized disclosure, modification or destruction.

PHI transferred between locations should be transported in a manner that protects the information from inappropriate review or disclosure.

Discussions related to clients should not be held in public locations to decrease incidental disclosures.

PC monitors that display PHI should be placed to ensure that confidential information is not readily accessible to unauthorized persons.

Visitors are escorted at all times by an authorized employee of the Department.

All persons in the Department wear appropriate identification to identify themselves.

All persons permitted access to the Department's computer systems are uniquely identified and access is limited to the minimum necessary PHI.

PHI is disposed in a manner to maintain the confidentiality of PHI and not to violate Policy 352.

FAX machines should be located in secure and controlled area so that information being displayed or printed is not visible to unauthorized observers.

FAX machines should be monitored at least every hour for receipt of PHI and PHI will be distributed or filed as addressed.

I. Policies and procedures (45 CFR 164.530(i))

POLICY 344: The Department implements policies and procedures with respect to PHI that are designed to comply with the requirements of the Privacy Rule and the Breach Notification Rule.

The Department's policies and procedures are reasonably designed to ensure such compliance, taking into account the size and type of activities that relate to PHI undertaken by the Department.

POLICY 346: Whenever there is a change in law that necessitates a change in the Department's policies and procedures required by the Privacy Rule or the Breach Notification Rule, the Department promptly documents and implements the revised policy or procedure. If the change in the law materially affects the content of the Notice of Privacy Practices, the Department must promptly revise the Notice of Privacy Practices in accordance with 45 CFR 520(b)(3).

POLICY 348: When the Department changes a privacy practice that is stated in the Notice of Privacy Practices and makes corresponding changes to its policies and procedures, it may make the changes effective for PHI that it created or received prior to the effective date of the notice revision because
the Department includes in its Notice of Privacy Practices a statement reserving its right to make such changes in its privacy practices. In implementing such a change, the Department will ensure that the changed policy or procedure, which was revised to reflect a change in the Department's privacy practice as stated in its Notice of Privacy Practices, complies with the Privacy Rule. The Department will document the policy or procedure, as revised, and revise the Notice of Privacy Practices. Unless otherwise required by law, the Department may not implement a change to a policy or procedure prior to the effective date of the revised Notice of Privacy Practices.

POLICY 350: The Department may change a policy or procedure that does not Materially affect the content of the Notice of Privacy Practices at any time, provided the changes are comply with the Privacy Rule and, prior to the effective date of the change, the policy or procedure, as revised, is documented.

J. Documentation (45 CFR 164.530(j))

POLICY 352: The Department must:

• Maintain the policies and procedures, pertaining to the Privacy Rule and the Breach Notification Rule, in written or electronic form;
• If a communication is required to be in writing, maintain such writing, or an electronic copy, as documentation;
If an action, activity or designation is required by the Privacy Rule to be documented, maintain a written or electronic record of such action, activity or designation
• Maintain documentation sufficient to meet the Department's burden of proof with regard to demonstrating that all breach notifications were made or that the use or disclosure did not constitute a breach, per 45 CFR 164.414.

• Retain the documentation required by the Privacy Rule and Breach Notification Rule for six years from the date of its creation or the date when it last was in effect, whichever is later.

SECTION IV Breach Notification Requirements (45 CFR 164.400 to 164.414, inclusive)

POLICY 400: Without unreasonable delay, and in no case later than 60 calendar days after the discovery of a breach of unsecured protected health information ("PHI"), the Department shall notify individuals whose unsecured PHI has been, or is reasonably believed by DSS to have been, accessed, acquired, used or disclosed as a result of such breach. A breach is considered to be discovered as of the first day on which it is known, or by exercising reasonable diligence, would have been known, to DSS. DSS is deemed to have knowledge of a breach if such 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 member of the workforce or an agent of DSS.

A. A breach means the acquisition, access, use or disclosure of PHI in a manner that is not permitted under the Privacy Rule which "compromises the security or privacy of the PHI."

B. The following situations are exclusions from the definition of a breach: unsecured PHI, meaning they do NOT rise to the level of a breach:

(1) Any unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of DSS or a business associate, if it was made in good faith, within the scope of authority and does not result in further use or disclosure in violation of the Privacy Rule.

(2) Any inadvertent disclosure by a person who is authorized to access PHI at DSS or a business associate, to another person authorized to access PHI at DSS or at a business associate, and the information received as a result of the disclosure is not further used or disclosed in violation of the Privacy Rule.

(3) A disclosure of PHI where DSS or business associate has a good faith belief that the unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

C. Except as provided in paragraph B above, an acquisition, access, use or disclosure of PHI in a manner not permitted by the Privacy Rule is **presumed to be a breach UNLESS** DSS or a business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

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

POLICY 401 Notifications to Individuals

A. If the Department determines that there has been a breach of unsecured PHI, the Department has specific obligations to notify the affected individual(s), the Secretary of Health and Human Services and possibly the media. Unsecured PHI means PHI that is not rendered unusable, unreadable or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary of Health and Human Services in the guidance issued under section 13402(h)(2) of Public Law 111-5 (the "Guidance"). See Appendix D.

If PHI is transmitted on paper or if it is transmitted by e-mail without the use of Tumbleweed or by CD without encryption specified in the Guidance, to an unauthorized individual, it is unsecured. If PHI is transmitted with the use of Tumbleweed and it is sent to the wrong person, i.e., to a person who is not the subject of the PHI or to a person who is not the authorized or legal representative of the individual who is the subject of the PHI, and the Tumbleweed e-mail is opened by this unauthorized person, DSS will treat this as a disclosure of unsecured PHI.

B. The notification to an individual must be written in plain language; sent by first-class mail to the individual at the last known address or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail; and contain the following information:

(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 PHI that were involved in the breach (such as whether full name, social security number, date of birth, home address, client number, diagnosis, disability 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 DSS is doing to investigate the breach, to mitigate harm to individuals and to protect against further breaches; and

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

The notification may be provided in one or more mailings as information is available.

C. If DSS knows the individual is deceased and it has the address of the next of kin or personal representative of the individual, it shall send written notification by first-class mail to either the next of kin or the personal representative. The notification may be provided in one or more mailings as information is available.

D. If there is insufficient or out-of-date contact information that precludes written notification to the individual, DSS shall use a substitute form of notice, reasonably calculated to reach the individual. Substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative of the individual.

(1) If there is insufficient or out-of-date contact information for fewer than 10 individuals, substitute notice may be provided by an alternative form of written notice, telephone or other means.

(2) If there is insufficient or out-of-date contact information for 10 or more individuals, then substitute notice shall be in the form of either

(a) a conspicuous posting for a period of 90 days on the home page of the DSS website; or
(b) a conspicuous notice in major print or broadcast media in the geographic areas where the individuals affected by the breach likely reside. Whether on the website or in the media, the notice must include a toll-free telephone number that remains active for at least 90 days where the individual may learn whether his or her

unsecured PHI may be included in the breach.

E. If DSS determines that the situation requires urgent intervention because of possible imminent misuse of unsecured PHI, DSS may provide information to individuals by telephone or other means, as appropriate, in addition to the notice provided above.

POLICY 402: Notification to the Media

Without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach that involves **more than 500 residents** of the state, the Department must also notify prominent media outlets serving state. The notification must meet the requirements in Paragraph B of Policy 401.

POLICY 404: Notification to the Secretary of Health and Human Services

Following the discovery of a breach of unsecured PHI, the Department must notify the Secretary of Health and Human Services as follows:

A. For breaches of unsecured PHI involving 500 or more individuals, DSS must notify the Secretary of Health and Human Services contemporaneously with the notice it sends to individuals and in the manner specified on the United States Department of Health and Human Services Web site.

B. For breaches of unsecure PHI involving fewer than 500 individuals, DSS must maintain a log or other documentation of such breaches. Not later than 60 days after the end of each calendar year, DSS must provide notification to the Secretary of Health and Human Services for breaches occurring during the preceding calendar year, in the manner specified on the United States Department of Health and Human Services Web site.

POLICY 405: All notifications required by the Breach Notification Rule will be issued from the Department's Office of Legal Counsel or by the Department's business associates, as determined by the Department.

POLICY 406: Notifications By Business Associates to the Department

The Department's business associates must notify the Department following the discovery of a breach of unprotected PHI without unreasonable delay and in no case later than 30 days following the discovery of a breach of unsecured PHI. A breach is considered discovered as of the first day on which it is, or reasonably should have been, discovered by the business associate. A business associate is deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the business associate.

A. The business associate shall include in its notification to the Department all of the elements required by its business associate contract with the Department and also any other available information that the Department is required to include in its notification to the individual at the time of the notification or promptly thereafter as the information becomes available to the business associate.

B. The business associate shall provide appropriate staffing and have established procedures to ensure that individuals who are informed by DSS of a breach of unprotected PHI by the business associate have the opportunity to ask questions and contact the business associate for additional information regarding the breach of unprotected PHI, in accordance with its business associate agreement.

C. The business associate shall comply with all other requirements of its contract and business associate agreement with the Department with regard to obligations in the event of a breach.

POLICY 408: If a law enforcement official states to the Department, or to a business associate of the Department, that a notification, notice or posting, as required above, would impede a criminal investigation or cause damage to national security, the Department or business associate shall delay the notification.

A. If the law enforcement official's statement is in writing and specifies the time for which a delay is required, the Department or its business associate shall delay such notification, notice or posting for the time period specified by the law enforcement official.

B. If the law enforcement official's statement is made orally, the Department or its business associate shall document the statement, including the identity of the official making the statement, and delay the notification, notice or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described above is submitted during that time.

POLICY 410: In the event of a use or disclosure in violation of the Privacy Rule at the Department, it is the Department's burden to demonstrate that all notifications were made as required by the Breach Notification Rule (regulations (Subpart D of Part 164 – Security and Privacy).

POLICY 412: The Department complies with the administrative requirements of: 45 C.F.R. 164.530(b) concerning training; 45 C.F.R. 164.530(d) concerning complaints to the agency for not following policies and procedures; 45 C.F.R. 164.530(e) concerning sanctions; 45 C.F.R. 164.530(g) concerning refraining from intimidation and retaliation; 45 C.F.R. 164.530((h) concerning non-waiver of rights; 45 C.F.R. 164.530(i) concerning maintaining policies and procedures; and 45 C.F.R. 164.530(j) concerning documentation with respect to the requirements of the Breach Notification Rule (Subpart D of Part 164 – Security and Privacy).

Procedures:

If a DSS workforce member believes that there has been a use or disclosure in violation of the Privacy Rule, the workforce member should contact his or her manager. The manager will obtain as much factual information as possible about the details of the improper use or disclosure: to whom and when was the disclosure made; was it a paper or electronic disclosure; if electronic, was Tumbleweed in use or was it within the State system firewall; what were the circumstances of the improper disclosure; what was the content of the PHI that was disclosed; whether steps may be taken to mitigate any known harmful effects of the improper disclosure; and any other relevant information. The manager shall take all reasonable steps to seek to have the improperly disclosed PHI returned to DSS or destroyed and shall ask the individual to whom the PHI was sent in error to send DSS a written statement indicating that he or she has not retained, copied or re-disclosed the PHI.

Within one business day of obtaining this information, the manager shall e-mail or fax this information to the DSS Privacy Officer or legal counsel to the Privacy Officer in Central Office.

Within one more business day, the manager and DSS Privacy Officer or legal counsel will review together the factual information and consider whether the matter qualifies as an "exclusion." If so, this shall be documented by the Privacy Officer or legal counsel. The incident shall be accounted for as a disclosure that was not for purposes of treatment, payment or health care operations.

The Privacy Officer will document his or her activity and conclusions with regard to the determining whether there a low probability that the PHI has been compromised based on a risk assessment of the factors set forth in Paragraph C of Policy 400 the Privacy Officer shall consult

with legal counsel and whomever he or she believes is appropriate and make a recommendation to the Commissioner about whether there was a "breach of unsecured PHI" and, if so, what type of notification is appropriate. If the Privacy Officer recommends that notification is required or appropriate and Commissioner accepts the recommendation, the Privacy Officer shall write the notification, in accordance with the requirements in federal law, and ensure that notification is performed in the manner specified by federal law. The Privacy Officer shall maintain a log of all breaches of unsecured PHI and shall submit said log to DHHS in accordance with the requirements of federal law.

The Privacy Officer shall also be responsible for receiving all reports breaches from the Department's business associates and reviewing the documented risk assessment performed by the business associates. If the business associate determined that there had been breach of unprotected PHI and the Privacy Officer agrees, the Privacy Officer shall recommend notification to the Commissioner. If the Privacy Officer disagrees with the risk assessment performed by the business associate and determines that there has not been a breach of unsecured PHI requiring notification, the Privacy Officer shall document his or her risk assessment and the reasons why he or she does not believe there has been a breach of unsecured PHI requiring notification to individuals