
THE GREAT SEAL OF THE STATE OF MONTANA
ORO Y PLATA

Table of Contents

Attachments

Information Security and Database Access Policy

I. Background:

The Department of Public Health and Human Services (DPHHS) is the designated single state agency responsible for the administration of: TANF, Foster Care, DD, Medicaid, Child Support & Welfare Services, Aging and Basic Support Programs, and numerous smaller programs assigned by Federal or State authority. In addition, DPHHS is the sole successor agency of those agencies previously providing these services. As such, program administration is defined to encompass all of the individual service areas under DPHHS' single agency jurisdiction. To properly administer these programs, the Department must collect vital records, information relative to the state's population and information on individuals and applicants for state services and benefits. This information is, in many cases, not releasable outside the actual collection unit without modification to preserve confidentially of client records or without proper authorization based on a "need-to-know" for purposes related to the administration of Departmental programs. DPHHS has the responsibility for ensuring that confidential information under the control of the Department are not compromised, while at the same time ensuring that the programs are properly administered. Therefore, it is essential that the Department establish a policy and process that will validate any request for access to privileged information against a framework of legitimacy criteria designed to test the appropriateness of the request.

II. Policy:

It is the policy of the Department of Public Health and Human Services to protect the confidentiality of the DPHHS client information and to ensure that access to such information is restricted to legitimate purposes of program administration. This policy is not intended to provide a barrier to program management. Although each employee is expected to abide by the letter of the policy and their signed confidentiality agreements, there may be situations where special circumstances or effective management requirements would indicate a need to deviate from this policy. In this event, Division Administrators should refer the situation to the DPHHS Director or his/her designee**,** with a request for a change or exception to the policy or an exception to an individual's confidentiality agreement. The governing principle that must be followed is that only the minimum necessary client information will be shared on a "need to know" basis that is in the best interest of the client, effective administration of the program and the health and safety of Montana's citizens.

III. Applicability:

Certain agencies and organizations outside of, but with ties to, the Department also have a legitimate "need-to-know" relative to some program information. These agencies are defined as any organization, either public or private:

(1) That the Department contracts for specific services;

(2) That has a legitimate need-to-know; and

(3) With which the Department has a Business Associate Contract or a Memorandum of Understanding to protect the confidentiality of the information.

The collective term for combined Department and "contract" agencies will be the "Department/Contractor organization". Agencies and individuals outside this organization also occasionally request such information and may have a legitimate need-to-know. This policy and process is therefore applicable to both the Department/Contractor organization and all other agencies and individuals.

IV. Scope:

This document is intended to address requests for and sharing of, on a need-to-know basis, all information compiled and maintained by any component of the Department/Contractor organization relative to individuals or groups of individuals served by the organization, or any information utilized in the administration and management of programs assigned to the Department. Such information may be contained in computer databases including mainframes, mid-tier computers and PCs, or non-automated data files. Requests may range from one time, individual requests for specific and limited information to requests for continuous, direct electronic access to an entire computer database. Requests may originate from components within the Department/Contractor organization other than the custodial component, or from any agency or individual outside of this organization. The scope of this document will cover all possibilities within this framework.

V. Administration:

Administration of the policy and process for controlling information distribution will be the responsibility of the Information Security Officer. The function of this person is to:

1) Review and process all requests for release information made by entities outside the Department/Contractor organization after appropriate Division approval**.**

2) Review and process all requests for release of information from the originating Division to other Department/Contractor organizations that are forwarded by the Division Administrators (or their designee) for processing, and all requests from non-DPHHS entities approved by the Division Administrator (or their designee);

3) Periodically review access policies that affect confidentiality of information.

In all cases within this policy where the Division Administrator is authorized to release client information, the Administrator concerned may delegate approval authority and establish written rules and procedures within the division as desired to facilitate effective program management and policy compliance. Any such written rules and procedures must bear the approval signature of the Division Administrator and shall be reviewed on an annual basis to ensure continued compliance with this policy and the associated HIPAA policies.

VI. Priority:

This policy is intended to provide guidance to maintain the confidentiality of client information in situations where no other policy exists. This policy does not preempt federal policies relative to any individual program under the administration of DPHHS. Federal policies shall have precedence over any provision of this policy. In that all requests for information or access to information are submitted to Division Administrators (or their designee) for approval or review and comment, Division Administrators shall ensure that all State and Federal confidentially requirements for programs under their purview are adhered to.

VII. Process:

Any process that controls dissemination of information must address the interests of the clients being served, on which the information are accumulated, as well as both the custodian and the requestor of the information. The process must also take into account the nature of the information involved in terms of the level of sensitivity relative to the privacy rights of the clients.

A. Sensitivity Levels:

In an effort to define categories of sensitivity on which to base access control measures, the following "sensitivity-levels" have been established

Level 1: This is information of a general nature about the characteristics of the population served by a program. Information is presented in such a way that individual clients cannot be identified from analysis of the information. Examples include: TANF population characteristics, such as average length of stay, mean payment level, and recidivism rate and; Medicaid client information such as the average age of clients, geographic distribution, and outcome analysis, such as relationships between preventive services and cost of care. Basically, Level 1 information represents information summary type information rather than individual-specific information.

Level 2: This is the client demographic and basic service information. Generally, Level 2 demographic information is program specific and is limited to information necessary to identify if an individual or family is known to the Department and to determine their program eligibility. Demographic information would be limited to name, address, phone number, date of birth and social security or other identification number. Service information would be limited to the type of service(s) received or being received, dates of service(s) and the component within the Department providing the service(s). Level 2 information is considered "Confidential" in that the fact that an individual or family is known to the Department and has received or is receiving services is controlled by the Department on a need-to-know basis, but is not considered to be "sensitive" information in terms of the following Level 3 definition.

Level 3: Information at this level is detailed information about an individual client's personal background or previous and present services provided by the Department. Level 3 information is considered as "sensitive" information in that if the information is improperly used, serious damage could occur to the individual or family concerned. Examples of Level 3 information would include medical status and history including past and present conditions or illnesses, specifics of medical diagnosis or tests, treatment plans, family background, child support requirements and status if

appropriate, financial status and specific information relative to the services provided by the Department. (See Section VII-B below for further definition.)

B. Determination of Sensitivity:

To be able to implement an access control process based on sensitivity-level classification, each Division must be able to determine the sensitivity levels associated with the client-specific information elements collected and maintained by the Division. By previous definition, individual information elements cannot, by themselves, be Level 1, in that Level 1 are summary information, or the sum, average, mean, etc. of many individual records of the same or combination of the same information element(s). All individual information elements therefore fall within Level 2 or Level 3 categories. For the purpose of structuring and administering this program, it will be sufficient to assume that those information elements that are not Level 3 will automatically be Level 2. The test for Level 3 classification is as follows: Any information element which, when taken together with client-identifying information elements would create "sensitive" information, is considered to be a Level 3 information element. An example of this would be a information element for medical diagnosis that shows "HIV positive", together with a name or other identifying element. This would identify a specific individual as being HIV positive, a fact that could be damaging to the individual if improperly used. This would make the medical diagnosis element "sensitive" and as such would be Level 3.

C. Sources of Information:

To administer this program all sources of information that are subject to sharing must be identified. Each Division Administrator (or their designee) shall determine a listing of all such sources, including information located on the state's mainframe, contractors' systems, the Department's mid-tier computer (RS6000), and all PC based programs, as well as all non-automated information files. These listings should include a brief description of the type, purpose and content of the information or file, where it is located and who the custodian and/or point of contact is. This information should be provided to the Administrator of the Operations and Technology Division (or their designee) for compilation and distribution and should be kept current at all times.

D. Requesting Information (Information):

1. **Requests for information from within the Department/Contractor organization:**
   Level 1 requests made to a component of the Department holding the information, by another component within the Department or from a contracting agency, will be in writing and must be submitted to the specific individual or component holding the information, or to the appropriate Bureau or Division. Division Administrators (or their designee) shall establish internal procedures and policies regarding the maintenance and release of Level 1 information, and may

designate selected staff members who have authority to release such information. Requests for Level 1 information may be made informally and verbally if desired.

Requests for Level 2 information must be submitted to and approved by the Division Administrator (or their designee) of the Division having custody of the information. Division Administrators are responsible for ensuring that information provided is no higher than Level 2 information.

Level 3 information requests must be submitted to and approved by the Division Administrator (or their designee) of the Division having custody of the information. However, these requests may be deferred, at the discretion of the Division Administrator, to the Director or his/her designee for final action.

Requests for Level 2 and Level 3 information must be in writing, utilizing the appropriate form. (See matrix in paragraph 3 below). All requests must include adequate justification for receiving the information and list the specific information elements requested.

2. **Requests for information from outside the Department/Contractor organization:**
Requests for Level 1 information from outside the Department/Contractor organization must be in writing, and must be submitted to the Data Owner of the information. Division Administrators (or their designee) shall establish internal procedures and policies regarding the maintenance and release of Level I information, including requirements for written requests as desired, and may designate selected staff members who have authority to release such information.

   Requests for Level 2 or Level 3 information must be in writing utilizing the "NON-DPHHS EMPLOYEE SYSTEM/FILE ACCESS REQUEST" form (DPHHS-OM-300B - attached). All Level 2 and Level 3 information requests must be initially submitted to the Division Administrator (or their designee) of the Division having custody of the information for review and comment prior to consideration by the Security Officer. (See matrix in paragraph 4 below).

   All requests must include adequate justification for receiving the information, an explanation of how the information will be utilized and a list of the specific information elements requested.

3. **Exceptions to Director Approval Requirements:**
To insure that the administration of Department programs is not negatively affected by this policy, the following situations are exempt from Director approval requirements:

a) The Division Administrator (or their designee) of the Division owning the information may approve requests from Department employees or Contractors' staff that require information to perform their assigned duties.

b) The Department Security Officer must approve requests from Department employees or Contractors' staff that requires online information access to perform their assigned duties, with oversight authority for the information involved.

c) Information which is required to link records from different information sets obtained from various Divisions, or to group records within a information set obtained from other Divisions, may be released by the Administrators of those Divisions (or their designee) in order to perform specific analyses for the purposes of public health research, assessment and assurance.

d) Requests for information by County Public Health agencies relative to their own county only may be approved by the Division Administrator (or their designee) of the Division owning the information. Typically, this are information that has been provided by the county, has been assimilated into the system, compiled and is being provided back to the originating county.

e) Approval for and confidentially of client information provided to medical service providers relative to individuals' eligibility and other essential information is covered in the HIPAA PRIVACY POLICY #002 (Attachment iii) and in the provider enrollment agreements.

f) Information may be released to one program in a DPHHS component by a different program in another DPHHS component where the two components have been asked to provide, or are providing, simultaneous services to the same client or family, and the process does not violate federal privacy and safeguard policy.

g) Information that has been determined to be a matter of public knowledge may be released by the Administrator of the Division (or their designee) having custody of the information. An example of this would be the names of parents delinquent in child support payments, with the amount owed.

h) Information may be released by Division Administrators (or their designee) to outside agencies or individuals where federal or state law requires or allows the sharing of information. Examples of this are: Sharing information on communicable diseases with

CDC; allowing access to TEAMS and SEARCHS databases to the Department of Justice for the purpose of fraud and abuse investigations; and providing information to individuals for purposes such as peer reviews. Division Administrators (or their designees) may provide a one time written authorization for routine, long term releasing of information to such Agencies or individuals by division personnel without written requests and approval for each occurrence. Such authorizations must be reviewed by Division Administrators (or their designees) on a semi-annual basis to maintain currency. In cases of releasing information to outside agencies, a memorandum of understanding with the outside agencies, or a signed DPHHS request form is required. For release of information to outside individuals, either a signed (information) request form as reflected above, or a separate, signed Business Associate Agreement is required.

4. Submission of Requests:

DPHHS or Contractor / Business Associate:

Sens. Level	Form(at)	Submit To	Approved By
1	Any Verbal or Written	Indiv/Div. Holding Info	Division Administrator or designee
2	DPHHS-OM-300A	Indiv/Div. Holding Info	Division Administrator or designee
3	DPHHS-OM-300A	Indiv/Div. Holding Info	Division Administrator or designee

Non-DPHHS or Contractor / Business Associate:

Sens. Level	Form(at)	Submit To	Approved By
1	Any Verbal or Written	Indiv/Div. Holding Info	Division Administrator or designee
2	DPHHS-OM-300B	Indiv/Div. Holding Info	Division Administrator or designee
3	DPHHS-OM-300B	Indiv/Div. Holding Info	Division Administrator or designee

Note: All requests must be submitted to the Administrator of the Division (or their designee) that has custody of the information for confirmation of sensitivity level and comments before forwarding to the Information Security Officer.

5. Information Security Officer:

An Information Security Officer will be assigned to provide support for this process.

The Information Security Officer will:

a. Receive all information requests being submitted.

b. Review requests and resolve any deficiency in form requirements;

c. Maintain all requests on file;

d. Make recommendations on policy changes;

e. Monitor the administration of this program, providing assistance as required;

Non-DPHHS agencies and individuals should contact Technology Services for proper forms and the initiation of the access process.

E. Approval of Information Requests:

Approval of information requests will be granted as follows for each level of information:

1. Level 1 information is neither confidential nor sensitive and is available to the general public on request. This is also the level at which information is provided to the legislature, news media, research organizations, and survey requests.

2. Level 2 information is considered to be confidential and is normally available to the entire Department/Contractor organization only on a need-to-know basis for purposes of program administration, case management, program coordination, or budgeting. The Division Administrator (or their designee) responsible for control of the information must authorize the release of Level 2 information for a specific client or family. Level 2 information may not be released outside the Department/Contractor organization without a signed release from the individual client (or their personal representative).

3. Level 3 information can only be released to any component of the Department/Contractor organization outside the originating division if the individual client (or their personal representative) signs a release form. Level 3 information can only be released to outside entities as specified by the client's signed release form. The criteria used to evaluate all requests for Level 3 information will include the requestors' specific need-to-know, potential benefit/detriment to the client(s) and impact on program effectiveness. Written approval of the request will be retained on file.

4. As indicated in the above two paragraphs. Level 2 and Level 3 information relative to an individual or a family may be released if the individual (or their personal representative) has signed the appropriate release form. In this event, the information to be released must be specifically authorized in the release form and must be released only for the purposes as indicated in the release form. This would include releasing information to other agencies in order to determine client eligibility and benefits, and to charitable organizations that may request names of individuals or families to contribute to on special occasions such as holidays. Division Administrators (or their designee) must authorize the release of such information by division staff members if a release form signed by the individual concerned is on file.

5. In cases where information to be released relative to an individual or family contains information originating from a third party, prior authorization to release such information must be obtained from the third party where the third party has sole ownership and has not provided previous release consent.

F. Appeals to denied request for information:

In cases where information requests from within the Department/Contractor organization are denied by the Division Administrator (or their designee) responsible for the security of the information, such denials may be appealed to the Director or his/her designee. All appeals must contain adequate justification for access and the consequences of not obtaining the information.

G. Cost of Providing Information:

The implementation of request for information from, or direct access to, information files under this policy may require special computer programming or other expenses to provide the specific information required while at the same time protecting confidential information that are not required. Such costs will normally be borne by the requestor as a condition for approval. The Department has developed a system change request process that will facilitate accomplishment of programming necessary to provide the desired information or access.

VIII: Direct, Electronic Access to Information:

Direct electronic access to information files required compliance with all of the rules listed above for the general sharing of information. However, the process involved in requesting and authorizing access is somewhat different and is covered in this section.

A. Access Request and Authorization Process:

1. Electronic access to information is granted on an individual basis only. All requests must be in writing. Requests from within the Department must use the DPHHS EMPLOYEE SYSTEM/FILE ACCESS REQUEST form (DPHHS-OM-300A - attachment i). Requests from Department Contractors or other agencies or individuals outside the Department must use the NON-DPHHS EMPLOYEE SYSTEM/FILE ACCESS REQUEST form (DPHHS-OM-300B - attachment ii).

2. Requests from outside or within the Department/Contractor organization will be approved by the authorized Data Owner (or their designee).

3. Information access requests will normally be preceded by verbal discussion involving appropriate staff supervisors of the requesting organization, the custodial organization and members of the Operations and Technology Division staff if required, the OTD Administrator will assign the request to the Security Officer for further analysis and consultation with the requesting agency. In these discussions, the nature of the access required will be ascertained and a specific contractor or Department representative will be assigned the responsibility of costing out the overall task of developing the linkages necessary to provide the requested access.

For all information systems access, the assigned representative will be an employee of the appropriate Division for the system.

All costs associated with providing the requested information are the responsibility of the requesting organization.

B. Security Procedures for Information Access:

DPHHS, in collecting and maintaining information belonging to the State of Montana, is responsible for ensuring that the information cannot be accessed by an unauthorized person, and cannot be accidentally or maliciously altered or destroyed.

The following rules and procedures regarding various aspects of security will be followed:

1. ACF2 Security Software The purpose of the ACF2 Security Software is to ensure the appropriate use of information and access to information residing on the state's mainframe computer.

2. Department Information Security Officer: The security officer:

    a. Maintains and is responsible for writing the ACF2 rules that allow access to specified information files;

    b. Reviews and implements all information access authorization request forms that have been signed by appropriate individuals and approved by the appropriate authority;

    c. Ensures that a unique Logon ID is assigned to individuals authorized for access to information files;

    d. Maintains a complete understanding of the current ACF2 security software capabilities, including future releases as they are implemented.

    e. Maintains copies of all security and control plans;

        i) A security and control plan will be completed by the Agency's Facility Maintenance contractor for each system based on contractual terms. Examples of Facility Maintenance contracted systems include TEAMS (The Economic Assistance Management System), CAPS (Child and Adult Protective System), SEARCHS (System for the Enforcement and Recovery of Child Support) and MMIS (Medicaid Management and Information System).

ii) Annual security and control plans will be completed by the Department for AWACS (Agency Wide Accounting and Client System), PHDS (Public Health Database System) and other information systems created or maintained by the Department.

f. Maintains copies of all risk assessments and analysis;

i) An annual risk assessment / analysis will be completed by the Agency's Facility Maintenance contractor based on contractual terms for TEAMS, CAPS, SEARCHS, MMIS, and other Facility Maintenance contracted systems to determine security threats to information and information resources for each system.

- Systems reviewed in the TEAMS plan will include CCUBS (Child Care and System), CHIP (Children Health Insurance Program), TESS (The Eligibility and Support System) and EBT system (Electronic Benefits Transfer).

ii) Annual risk assessment will be completed by the Department for the AWACS, PHDS and other information systems created or maintained by the Department.

3. Information File Owner: The Department Director is the "owner" of all information files for DPHHS; however, all of the security duties of the "owner" have been delegated to the Department Administrators (or their designee). As the designated agent for the Department Director, the Administrator:

a. Is responsible for determining who should be allowed access to each information file and the level of access;
b. Is responsible for approving access authorization request forms for persons permitted access to a information file;
c. Will notify the security officer of security requirements for new and existing information files;
d. Will determine the appropriate sharing of information with other agencies.

C. Security Procedures for Terminating or Modifying System Access:

The following rules and procedures regarding terminating or modifying system access will be followed:

1. Upon termination of employment with DPHHS, a DPHHS-OM-300A must be submitted by the employee's immediate supervisor asking that all system access be deleted. The Security Officer reviews current access and appropriate action is taken to terminate access previously granted.

2. When an employee modifies or changes their position within the agency, a DPHHS-OM-300A must be submitted requesting the appropriate access change;

3. For all non-DPHHS employees, a DPHHS-OM-300B must be submitted to the Agency Security Officer requesting deletion of system access or noting the changes that would require access modification.

IX. Employee Confidentiality and Consent Agreements:

Each and every employee of DPHHS that has an occasion and/or need to compile from and on an individual or group of individuals, obtain from other sources from within the organization, view, store, or otherwise handle or utilize any information that is considered Confidential (Level 2) and/or Sensitive (Level 3) regarding such individuals or groups of individuals served by the Department, shall sign a DPHHS EMPLOYEE SYSTEM/FILE ACCESS REQUEST form which contains a confidentiality agreement and will be maintained by the Security Officer. It is the responsibility of the respective Division Administrators to ensure all such employees have signed and do understand such an agreement and that these agreements are forwarded to the Security Officer.

Attachment i.

DPHHS EMPLOYEE SYSTEM/FILE ACCESS REQUEST
(DPHHS-OM-300A)

DPHHS-OM-300A
(Rev. 2/03)

STATE OF MONTANA
Department of Public Health and Human Services

Clear Form

DPHHS EMPLOYEE SYSTEM/FILE ACCESS REQUEST

Name of Individual Requiring Access: (Please Print) _____

Social Security Number: _____ Phone: _____

Logon ID: _____ Create Logon ID: ☐ Yes Delete Logon ID: ☐ Yes

Department: _____ Division/Bureau: _____

Address: _____ County: _____

_____

Access to: _____ is requested.

(e.g., TEAMS, CAPS, PJUSTICE, AWACS, TSO, CICS, etc.)

If applicable, enter the required security class or security codes: _____

Justification: *(Give a brief description as to why access is needed.)*

List File Access:

CONFIDENTIALITY/CONSENT STATEMENT: *(To be read and signed by the individual requiring access.)*

I hereby certify that I am entitled to the confidential client information to which I am requesting access. I will not release the confidential information to others unless it is for purposes directly connected to the administration of the program for whose purposes it was originally provided. Further release of this information may only be done upon authorization by the client whose privacy interest is involved or it may be released to others if specifically permitted by law. I understand that a violation of this policy will subject me to disciplinary action, which may include termination of my employment from DPHHS. I have read the DPHHS Internet Policy and the State of Montana's Computer Use Policies and I agree to comply with all terms and conditions. I agree that all network activity conducted while doing State business and being conducted with State resources is the property of the State of Montana. I understand that the State and Department reserve the right to monitor and log ***all*** network activity including E-mail and Internet use, with or without notice, and therefore, I should have no expectation of privacy in the use of these resources.

Signature of Employee: _____ Date: _____

Print Name of Supervisor: _____

Signature of Supervisor: _____ Phone: _____ Date: _____

System Representative: _____ Date: _____

Security Officer: _____ Date: _____

Attachment ii.

NON-DPHHS EMPLOYEE SYSTEM/FILE ACCESS REQUEST
(DPHHS-OM-300b)

DPHHS-OM-300B
(Rev. 2/03)

STATE OF MONTANA
Department of Public Health and Human Services

Clear Form

NON-DPHHS EMPLOYEE SYSTEM/FILE ACCESS REQUEST

Name of Individual Requiring Access: (Please Print) _____

Social Security Number: _____ Phone: _____

Logon ID: _____ Create Logon ID: ☐ Yes Delete Logon ID: ☐ Yes

Agency: _____ Division: _____

Address: _____

_____

Access to: _____ is requested.

(e.g., TEAMS, CAPS, PJUSTICE, AWACS, TSO, CICS, etc.)

If applicable, enter the required security class or security codes:

Justification: *(Give a brief description as to why access is needed.)*

List File Access:

CONFIDENTIALITY/CONSENT STATEMENT: *(To be read and signed by the individual requiring access.)*

I hereby certify that I am entitled to the confidential client information to which I am requesting access. I will not release the confidential information to others unless it is for purposes directly connected to the administration of the program for whose purposes it was originally provided. Further release of this information may only be done upon authorization by the client whose privacy interest is involved or it may be released to others if specifically permitted by law. I understand that a violation of this policy will subject me to disciplinary action, which may include termination of my employment from DPHHS. I have read the DPHHS Internet Policy and the State of Montana's Computer Use Policies and I agree to comply with all terms and conditions. I agree that all network activity conducted while doing State business and being conducted with State resources is the property of the State of Montana. I understand that the State and Department reserve the right to monitor and log ***all*** network activity including E-mail and Internet use, with or without notice, and therefore, I should have no expectation of privacy in the use of these resources.

Signature of Employee: _____ Date: _____

Print Name of Supervisor: _____

Signature of Supervisor: _____ Phone: _____ Date: _____

Supervisor: Access for this individual is allowed for six months. I realize I will have to contact the DPHHS Security Officer if this employee needs access beyond the six months. I understand that it is my responsibility to inform the DPHHS Security Officer immediately when this employee terminates or no longer needs access.

DPHHS Administrator: _____ Date: _____

Security Officer: _____ Date: _____

Attachment iii.

USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION

Department of Public Health and Human Services (DPHHS)

Health Insurance Portability and Accountability Act ("HIPAA") Privacy Policy

John Chappuis, Deputy Director

Date: February 27, 2003
Revised Date:

Policy Title:	Uses and Disclosures of Protected Health Information		
Policy Number:	002	**Version:**	1.0
Approved By:	John Chappuis		
Date Approved:	February 27, 2003		

Purpose:

This policy addresses the use and disclosure of Protected Health Information ("PHI") in order to provide necessary services and benefits to clients while maintaining reasonable safeguards to protect their PHI.

Policy:

DPHHS will limit uses and disclosures of PHI to those uses and disclosures which are required or allowed by law or are authorized by the client.

Required Disclosures – DPHHS is required to disclose PHI:

1. To the client, with certain specific limitations.

    a. When such disclosure, in the belief of the licensed health care professional, would be likely to cause harm;

    b. When DPHHS does not have the information; and

    c. When the professional believes that such disclosure might cause potential harm to other individuals.

2. To the Secretary of Health and Human Services when required to investigate or determine the Department's compliance with the HIPAA regulation.

Permitted disclosures without Authorization – DPHHS may disclose PHI without the client's authorization to the extent necessary for the following purposes:

1. Treatment – Provision, coordination or management of health care and related services by one or more health care providers, including the coordination or management of healthcare by a healthcare provider with a third party; consultation between healthcare providers relating to a client; or the referral of a client for healthcare from one health care provider to another.

2. Payment – The activities undertaken to determine or fulfill responsibilities for coverage and provision of benefits including: determination of eligibility or coverage; risk adjusting amounts due to health status or demographics; billing or collecting; obtaining payment for reinsurance purposes and all related data processing; review of health care services with respect to medical necessity, coverage, justification or appropriateness of care; and/or utilization review activities including precertification and preauthorization.

3. Healthcare Operations – Those business and management activities necessary to accomplish health care functions, including, but not limited to:

    a. Quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines;

    b. Reviewing the competence of qualifications of health care professionals, accreditation, certification, licensing or credentialing activities;

    c. Underwriting or premium rating;

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

    e. Business planning and development such as cost management, formulary development and payment or coverage policies; and/or

    f. Customer service provisions.

Uses and disclosures permitted or required by state or federal law for which a written authorization is NOT required (in most cases, these disclosures will need to be kept in an accounting log):

1. To Business Associates who conduct health care activities on behalf of a DPHHS entity and who provide assurances that the PHI will be safeguarded.

2. For public health activities related to the prevention or control of diseases, injuries or disabilities, including surveillance, vital events such as birth and death, public health investigations and interventions.

3. To a government authority authorized to receive reports of child or adult abuse or neglect or domestic abuse. If DPHHS staff makes such a disclosure, they must promptly inform the client that such a report has been or will be made, unless they believe that informing the

client or the client's personal representative would place that client or another individual at risk of serious harm. These disclosures are required from most health care professionals (MCA 52-3-811).

4. To report adverse events regarding food and drugs.

5. To workers compensation regarding work related injuries.

6. To health oversight agencies such as government regulatory bodies who determine program standards, eligibility and compliance.

7. To administrative or judicial proceedings in response to a subpoena or court order. Where federal or state law requires a court order for disclosure of specific information, that information will not be released without that court order.

8. For limited law enforcement activities, such as reporting certain injuries or wounds, identifying or locating a suspect, victim or witness, alerting law enforcement of a death as a result of criminal conduct, and information which constitutes evidence of criminal conduct on DPHHS premises. Montana law (MCA 50-16-530(4)) requires an investigative subpoena to make such disclosures.

9. To coroners or medical examiners, for the purpose of identifying a deceased person or determining a cause of death

10. To funeral directors, consistent with applicable law, as needed to carry out their duties regarding the decedent. DPHHS may also disclose such information prior to, and in reasonable anticipation of, the death. **Montana law (MCS 50-16-530 allows for these disclosures and will not interfere with disclosures required for death certificates.**

11. To organ procurement organizations or other entities engaged in procuring, banking, or transplanting of cadaver organs, eyes, or tissue, for the purpose of facilitating transplantation.

12. For research purposes with the approval of an Institutional Review Board (IRB).

13. To avert a serious threat to health or safety, if DPHHS believes such information is necessary to prevent or lessen a serious and imminent threat.

14. For other specialized government functions related to lawful intelligence, counterintelligence or other national security activities.

15. To a correctional institution having lawful custody of an inmate for the purpose of providing health care or ensuring the health and safety of clients or other inmates or protecting the safety, security and good order of the institution.

16. In case of emergency, DPHHS may use or disclose information to the extent needed to provide emergency treatment.

17. Government agencies administering public benefits may share information between government agencies to determine eligibility or to coordinate benefits and may maintain such information in a single or combined data system if such sharing is permitted or required by statute or regulation.

18. The Family Educational Rights and Privacy Act (FERPA) and state law applicable to student records governs access to, use, and disclosure of student records.

Uses and disclosure for which a client's authorization is not required if they are informed in advance and given a chance to object.

There are some circumstances in which DPHHS may disclose PHI without authorization if the person is informed in advance and is given an opportunity to agree or disagree or to restrict the disclosure. Except as otherwise provided by law, DPHHS may orally inform the client of and obtain the client's oral agreement or objections and must document this occurrence. These circumstances are:

1. For maintaining a directory of clients in a DPHHS health care facility. State law (MCA 50-16-530) restricts this disclosure to the patient's presence and a general condition;

2. For disclosure of health care information to a family member, other relative, or close personal friend of the client, or any other person named by the client, subject to limitations; and

3. Oral permission to use or disclose information for the purposes described in this Section is not sufficient when the client is referred to or is receiving substance abuse treatment services or mental health treatment services, where written authorization for the program to make such disclosures is required.

Uses for which a written Authorization IS required

1. Except as otherwise permitted or required by law and consistent with these policies, DPHHS shall obtain a completed and signed Authorization for release of information from the client, or the client's personal representative, before obtaining or using information about a client from a third party or disclosing any information about the client to a third part. An Authorization is required:

    a. Prior to a client's enrollment in a DPHHS administered health plan, if necessary for determining eligibility or enrollment;

    b. For the use and disclosure of psychotherapy notes and addiction treatment notes (42 CFR). Psychotherapy notes and addiction treatment notes are notes that are recorded in any medium and kept separate from the rest of the medical record by a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session. Psychotherapy notes

do not include 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;

c. For disclosures to an employer for use in employment related determinations; and

d. For research purposes unrelated to the client's treatment.

2. DPHHS may obtain, use, or disclose information only if the written Authorization includes all the required elements of a valid Authorization. The required elements are:

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

   b. The name or other specific information about the person(s) classification of person(s), or entity (such as DPHHS specified program) authorized to make the specific use or disclosure;

   c. The name or other specific identification of the person(s), classification of person(s), or entity to whom DPHHS may make the requested use or disclosure;

   d. A description of each purpose of the requested use or disclosure. If the client does not wish to specify a purpose for the information, they may specify "at the request of the client";

   e. An expiration date, or an expiration event that relates to the client or to the purpose of the use or disclosure. If a date is not included, the Authorization expires in 6 months. No expiration event or date can be listed that is greater than 30 months;

   f. Signature of the client or of the client's Personal Representative ("Representative") and the date of the signature; and

   g. If the client's Representative signs the Authorization form instead of the client, a description or explanation of the Representative's authority to act for the client, including a copy of the legal court document (if any) appointing the Representative, must also be provided.

3. Prior to any permitted disclosures, DPHHS must verify the identity of the person requesting the client's PHI and the authority of that person to have access to the PHI.

4. DPHHS must provide the client with a copy of the signed Authorization form.

5. DPHHS must document and retain each signed Authorization form for a minimum of six years and three months.

6. Uses and disclosures must be consistent with what the client has authorized on the signed Authorization form. Under any such authorization, DPHHS will disclose only the minimum amount of PHI necessary to fulfill the purpose for which the PHI is requested.

7. An Authorization must be voluntary. DPHHS may not require the client to sign an Authorization as a condition of providing treatment, payment, services, enrollment in a health plan or eligibility for health plan benefits, except:

    a. Before providing research related treatment, a DPHHS health care provider may condition the client to sign an Authorization for the use or disclosure of health information for such research;

    b. Before enrolling the client in a DPHHS health plan, DPHHS can condition the client to sign an Authorization if needed to help determine the applicant's eligibility for enrollment and the Authorization is not for the use or disclosure of psychotherapy notes; and

    c. DPHHS and its contracted health care providers can condition the client to sign an Authorization before providing health care that is solely for the purpose of creating protected health information for disclosure to a third party. For example, in a juvenile court proceeding, where a parent is required to obtain a psychological evaluation by DPHHS, the evaluator may, as a condition of conducting the evaluation, require the parent to sign an Authorization to release the evaluation report (but not the underlying psychotherapy notes) to DPHHS.

8. An authorization that is required for enrollment in a health plan or to determine eligibility for benefits or the health plan cannot be combined with a voluntary authorization. A required authorization and a voluntary authorization must be separate documents, signed separately.

9. Clients have a right to restrict the uses and disclosures of information. Such restrictions must be submitted in writing and do not affect disclosures that have already taken place in good faith.