HIPAA Introduction

When preserving confidentiality, the Department must also adhere to the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Congress recognized that advances in electronic technology could erode the privacy of health information. Accordingly Congress incorporated into HIPAA provisions that mandated the adoption of Federal privacy protections for individually indentifiable health information.

The U.S. Department of Health and Human Services published a final regulation in the form of the Privacy Rule in December 2000, which became effective on April 14, 2001. This rule set national standards for the protection of health information. DPHHS declared itself a single covered entity. Single covered entities must have implemented standards to protect and guard against misuse of individually identifiable health information by the implementation date, April 14, 2003. Additional HITECH regulations were implemented April 2005 safeguarding electronic protected health care information.

The U.S. Department of Health and Human Services issued the Omnibus effective March 26, 2013. The Omnibus provided changes in the following areas: 1) Makes business associates of covered entities directly liable for some HIPAA compliance requirements; 2) Strengthens limitation on the use and disclosure of PHI for marketing and fundraising purposes; 3) Expands individuals' rights to receive electronic copies of their PHI and permit restriction of sharing for services paid for out-of-pocket in full; 4) Required modification to the covered entity's Notice of Privacy Practices; 5) Modifications to the Authorization to facilitate research, disclosure of immunization proof to schools; 6) Allowing decedent information to go to family members or others; and 7) Enforcement of noncompliance with HIPAA rules due to willful neglect (changes to penalties) and civil penalties may be imposed due to willful neglect.

Statute

45 CFR Parts 160 and 164, Health Insurance Portability and Accountability Act

HIPAA Definitions

The following definitions apply to disclosure or access to HIPAA information maintained by the Department:

BUSINESS ASSOCIATE means a person or organization that performs a function on behalf of the Department that requires the use or disclosure of protected health information and relates to the health care component activities of the Department. Such functions

include claims processing, utilization review, quality assurance, billing, benefits management, legal, actuarial, accounting, consulting, data aggregation, management, administration, accreditation, patient safety or financial services. Business associates do not include members of the DPHHS workforce. An example of a business associate is a foster care contractor.

DISCLOSURE under HIPAA means the release, transfer, provision of, access to or divulging in any other manner of information outside the entity holding the information.

DUTY TO NOTIFY means when unsecured protected health information (PHI) has been released or a breach of PHI has occurred and poses a significant threat to the individual's privacy and security, based upon the risk assessment results, notification may be required to the individual involved, local or statewide media, and the Secretary of Health and Human Services. (DPHHS Policy #16 (Duty to Notify), is located on the DPHHS OURS website (front page, and click the HIPAA link, and then click the Policies link)

HEALTH CARE PROVIDER under HIPAA means a provider of medical or health services as defined in 42 USC 1395x(s), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

HEALTH INFORMATION per the Health Insurance Portability and Accountability Act (HIPAA) means any information, whether oral or recorded in any form or medium, that is created by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse that:

- Relates to the past, present, or future physical or mental health or condition of health care to an individual; or

- Relates to the past, present, or future payment for the provision of health care to an individual.

INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION is a subset of Health Information including demographic information, collected from an individual that is created or received by a health care provider, health plan, employer, or health care clearinghouse that:

- Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; and
- Relates to the past present, or future payment for the provision of health care to individual; and
- Identifies the individual; or
- There is a reasonable basis to believe the information can be used to identify the individual.

HIPAA means **HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA)**. This includes the U.S. Department of Health and Human Services publication of a final regulation in the form of the Privacy Rule in December 2000, which became effective on April 14, 2001. This rule set national standards for the protection of health information. By the compliance date of April 14, 2003, covered entities must have implemented standards to protect and guard against the misuse of individually identifiable health information.

PERSONAL REPRESENTATIVE means under the HIPAA Privacy Rule, a person authorized to act on behalf of the individual in making health care related decisions, which may include disclosure of the individual's protected health information.

PROTECTED HEALTH INFORMATION (PHI) means Individually Identifiable Health Information that is transmitted electronically in any medium or maintained in any medium. PHI does not include educational records covered by the Family Educational Right and Privacy Act, 20 USC 1232, the student records held in post-secondary institutions or the records of students 18 years or older. PHI also does not include employment records held by DPHHS in its role as employer.

- All PHI located in the case records containing reports of child abuse or neglect may be considered the Division's Designated Record Set under HIPAA.

  A **DESIGNATED RECORD SET** means 1) A group of records maintained by or for a covered entity that is:
  - The medical records and billing records about individuals maintained by or for a covered health care provider;
  - The enrollment, payment claims adjudication, and

case or medical management record systems maintained by or for a health plan; or

- Used, in whole or in part, by or for the covered entity to make decisions about individuals.

The term *record* means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used or disseminated by or for a covered entity.

RISK ASSESSMENT means Department staff will conduct a risk assessment when protected health information (PHI) is accidently, inadvertently, or through employee error disclosed. It is a DPHHS Risk Assessment Tool that contains 15 questions to be answered related to unsecured PHI, minimum necessary, significant risk, types and amounts of PHI involved, specific breach definition exclusions, and burden of proof. (Located on the DPHHS OURS website (front page, and click the HIPAA link, and the Risk Assessment link)

Department Staff Responsibilities regarding HIPAA

Each employee is responsible for his or her own actions and for knowing and understanding the agency's policies and laws concerning HIPAA. Each employee will receive orientation on HIPAA policy within 60 days of employment, and thereafter as necessary for the duration of employment.

All Department employees shall comply with Department policies concerning the uses and disclosures of PHI. **Any use or disclosure in violation of these policies will be subject to disciplinary action up to and including termination of employment as set forth in Policy Section 501-3.**

Supervisory Responsibilities, New Employee Orientation

The supervisor is responsible for assuring that each employee receives:

Orientation to relevant department per the new employee packet and according to CFSD MCAN training requirements.

Licensure Staff

Licensure staffs are responsible for ensuring that facilities and providers are informed of HIPAA requirements at the time of licensure.

Grant Administrators/ CFSD Contract Liaisons

CFSD Grant Administrators and Contract Liaisons are responsible for ensuring that contractors are advised of and agree to comply with HIPAA requirements prior to or at the time of execution of the contract.

- Violation of Department policy on HIPAA policy by a contractor may result in cancellation of the contract.

Duty to Report

Each DPHHS Employee or Contractor must immediately report any disclosure of PHI, in violation of federal and/or state law and rule requirements to their immediate supervisor or designee, the DPHHS Privacy Officer and if applicable, the Grants Administrator, the Contract Liaison, and/or the division liaison.

HIPAA Disclosures

Prior to releasing information from the case record, a written authorization must be signed by the individual who is either the subject of the protected health information or by his/her authorized representative, or disclosure must be otherwise permitted by law or ordered by the Court (including Tribal Courts).

HPS-401 Designation of Authorized Personal Representative for Health Information

The DPHHS form, HPS-401 (Designation of Authorized Personal Representative for Health Information), must be completed when a parent designates the authority to another person to receive and act on the individual's behalf and share the parent's PHI. A copy is provided to the individual and the original is filed in the case record, and will be scanned and attached to DocGen. SEE sample form at the end of this policy; the HPS-401 form is also located on the DPHHS OURS website (front page, and click the HIPAA link, then click the Forms link).

DPHHS as the Individual's Authorized Personal Representative (HIPAA)

NOTE: When the Court designates the Department to be the individual's personal representative as set forth in the Federal Health Insurance Portability and Accountability Act (HIPAA) regulations, the Department will self-authorize the release of protected health information regarding that individual as deemed minimally necessary to meet that individual's needs, in accordance with all other applicable federal and state statutes and rules.

Written Authorization

CFSD Authorization form CFS-210 meets the requirements of a valid HIPAA authorization for the disclosure of protected health information (PHI). The purpose of this form is to allow CFSD employees to share an individual's PHI outside the department (minimum necessary).

Individual's Right to Request File Type and Format

- The 2013 Omnibus HIPAA Final Rule provides individual with the right to choose the method for releasing electronic copies of his/her PHI, including the file type (e-mail, text, file transfer) and format (PDF, rich text). This right extends to sharing PHI with authorized third party recipients.
    - The release of PHI adheres to the guidelines found in CFSD and DPHHS confidentiality statute including CFSD 502-3.
    - CFSD staff shall obtain a written request that includes:
        - The individual's chosen method for sending PHI; format (e-mail, fax, file transfer) and file type (PDF, rich text) being requested.
        - Specification of what PHI is being requested
        - Documentation of the recipient's name and contact information (e-mail address….)
        - Acknowledgement of the inherent risk related to utilizing the chosen method, and the individual's knowledge of file transfer.
        - The individual's signature and date signed.
    - CFSD staff must offer alternative methods for sending PHI if the chosen method is not available using CFSD resources.
    - The preferred method of sending electronic PHI is through the State of Montana file transfer system. Under HIPAA, CFSD staff is required to inform individuals if the method they have chosen is not secure.

      (Note: The inherent risk with utilizing an insecure file type is included on the CFS-199, and provided to each adult individual with whom we work.)

CFSD Dissemination of PHI with appropriate file type and/ or by De-identifying the PHI.

Although the 2013 Omnibus permits the "youth's legal representative" to utilize discernment and choose the file type (e-mail, text) and format (rich text, PDF) in which to disclose PHI, the DPHHS Security Rules states, "In drafting or sending e-mail messages, employees should not include anything that would not be appropriate for dissemination to the public. E-mail communication must reflect professional and respectful business correspondence. Electronic communications will be monitored for performance, trouble-shooting purposes, and detection of abuse. In addition, employees should use their best judgment in sending messages that contain information required by law to be confidential." CFSD staff must use discernment on a case by case basis when using

insecure file types for sharing PHI. As servants of the public, CFSD staff is obligated to act within our capacity to assist individuals, timely responses concerning imminent child abuse/ neglect and/or life threatening situations may merit utilization of insecure file types containing PHI. Staff shall follow CFSD and DPHHS confidentiality statute including CFSD 502-3 and the Security Rule. Whenever possible staff shall:

- Utilize file transfer (DPHHS's only secure electronic method)

OR when choosing an insecure method

- De-Identify (use medical ID #, Caps ID, Case ID, Initial)
- Redact content or individual identifiers (take out addresses and only send minimal necessary)
- Verify the recipient's electronic contact prior to sending

https://dphhs.mt.gov/tsd/internetintranetpolicy

Complaints and Violations regarding HIPAA Disclosures

Every complaint regarding an alleged violation of HIPAA policies shall be promptly investigated by the immediate supervisor, and others involved in the assessment risk of harm to the individual(s).

Complaint Process

All HIPAA privacy complaints must be reported to the DPHHS Privacy Officer. Written complaints will be reported by mailing or faxing the complaint to the DPHHS Privacy Officer. Verbal and telephone complaints will be referred directly to the Privacy Officer, who will attempt to resolve the matter. The Privacy Officer will coordinate the effort to resolve complaints with the appropriate supervisor, and others involved in the assessment of the complaint. MAILING ADDRESS: DPHHS Privacy Officer, PO Box 202960, Helena, MT 59620-2960.

DPHHS PHI Complaint Form

If the problem cannot be immediately solved, the individual will be asked by the DPHHS Privacy Officer if he/she would like to file a formal complaint. If so, the individual will be encouraged to use the Protected Health Information (PHI) complaint form. This form is available electronically on the Department's OURS website (front page, and click the HIPAA link, and the Forms link)

The complaint must contain a short and plain statement of each reason the complainant contends that DPHHS employees of the State or Business Associates of the State have violated policies and procedures relating to the uses and disclosures of PHI.

Privacy Officer Response to Complainant

The Privacy Officer will contact the Complainant to determine if a resolution to the problem can be developed. The Privacy Officer will document unsuccessful attempts to contact the Complainant. A complaint file will be maintained by the Privacy Officer containing each complaint and its resolution. CPS case records shall be kept for a minimum of twelve (12) years. Other records that contain PHI must be maintained for a minimum of six years and three months.

Complaints alleging violations of HIPAA policies by personnel of the Department will be referred to the Office of Human Resources. The Privacy Officer will follow up with that office to ensure the issue has been resolved.

Resolution of complaints will be documented on the complaint form. The Privacy Officer will send written notice to the complainant explaining how the problem was resolved. This notification shall also inform the complainant that he/she has a right to file a complaint with the Office for Civil Rights of the U.S. Department of Health and Human Services and shall include applicable contact information.

- Complaints related to other covered entities' uses and disclosures of PHI shall be referred to that entity's Privacy Officer and/or the Office of Civil Rights (Washington D.C.) at:

U.S. Department of Health and Human Services
Office for Civil Rights
200 Independence Avenue, SW – Room 506-F
Washington D.C. 20201
(866) 627-7748

Complaints not related to HIPAA privacy but related to other business practices will be referred to the appropriate program or management staff for resolution of the complaint.

DPHHS Risk Assessment Tool

The DPHHS Risk Assessment Tool must be completed for each occasion when PHI is accidently, inadvertently or through employee error disclosed. If the nature of the PHI released poses a significant risk of financial harm, reputational or other harm the violation will be considered a breach. The results will be sent to the DPHHS Privacy Officer, who will document the findings for the HIPAA record. The DPHHS Risk Assessment Tool is located on OURS (link on the home page).

If the determination is made through the DPHHS Risk Assessment Tool that a breach of PHI has occurred, and risk of harm exists to the individual whose PHI was released, then the steps provided in DPHHS Policy #16 (Duty to Notify) will be followed to ensure appropriate risk management measures are taken.

Duty to Notify

When unsecured protected health information (PHI) has been released or a breach of PHI has occurred, and poses a significant threat to the individual's privacy and security, based upon the risk assessment results, notification by the Department may be required to the individual involved, local or statewide media, and the Secretary of Health and Human Services.

NOTE: The Division Administrator, in coordination with the Department Director's Office will determine who will be notified, and how a notification will occur, when it is required.

Log Accounting for Disclosures

If the division liaison was not made aware of the complaint, and a disclosure was made, the person who made the disclosure or his/her supervisor will advise the division liaison, and the DPHHA Privacy Officer. The division liaison and Privacy Officer, along with field staff associated with a disclosure cooperatively work together to asses, mitigate, and document facts surrounding the disclosure utilizing the Risk Assessment Tool. The Risk Assessment Tool is found on OURS and applies Federal Regulations regarding PHI disclosures.

Other Penalties

In addition to an individual employee possibly being subject to disciplinary action up to and including termination of employment as set forth in Policy Section 501-3, HIPAA violations are subject to financial penalties as determined by the U.S. Office for Civil Rights. The Department could be subject to fines ranging from $100 - $50,000 per incident, up to $1.5 million annually (all such violations of an identical provision). If willful negligence is determined to have taken place, the Department could be subject to fines ranging from $10,000 - $50,000 per incident, up to $1.5 million annually (all such violations of an identical provision), and civil penalties may be imposed due to willful neglect.

Rev. 10/03
Rev. 10/05
Rev. 10/06
Rev. 10/07
Rev. 10/10
Rev. 10/11
Rev. 11/14