DPHHS EMPLOYEE TRAINING

HIPAA (HEALTH INSURANCE PORTABILITY & ACCOUNTABILITY ACT)

ARRA (AMERICAN RECOVERY & REINVESTMENT ACT)

HIPAA

- HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (Kennedy/Kassebaum bill of 1996) April 14, 2003 HIPAA became part of our everyday life. We all have had to sign HIPAA statements at our doctor's and/or dentists offices or at a health care clinic.
- HIPAA law protects the privacy and security of everyone's protected health information (PHI). Information that deals with our names, addresses, email address, photographs or other pictures, doctor visits, diagnosis and other items that identify us.

HIPAA

- As employees of the Department of Public Health and Human Services (DPHHS) you are part of a covered entity under HIPAA.
- As a covered entity all employees are responsible for the protection of the privacy and security of our clients/patients/recipients.
- There are penalties associated with using, abusing and disclosing protected health information. You can be fired from your job, fined up to $25,000.00 per year, and you can be sentenced to jail time if you knowingly and willingly use and abuse a clients PHI.

ARRA

- ARRA has added penalties to HIPAA law. There are additional requirements for reporting disclosures; business associates are going to be responsible for disclosures they make; and individuals will need to be notified if there is a disclosure, or breach, of their PHI.
- DPHHS as a covered entity has identified breach notification criteria and is developing training to mitigate breaches of protected health information by employees or business associates.

ARRA

- BREACH NOTIFICATION FOR UNSECURED PROTECTED HEALTH INFORMATION:
- BREACH: "The unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information."
- UNSECURED PROTECTED HEALTH INFORMATION: "Protected health information that is not secured through the use of a technology or methodology specified by the Secretary in guidance" (Secretary of Health and Human Services)

ARRA

- Guidance by the Secretary: Specific technologies and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals.
- Those technologies are ‘encryption’ using a NIST (National Institute of Standards and Technology) verified encryption technology. This applies to data at rest, data in motion and data in use.

ARRA

- Media on which the PHI is stored or recorded has been destroyed in one of the following ways:
  - 1. Paper, film or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise reconstructed. Redaction is specifically excluded as a means of data destruction.
  - 2. Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800-88 such that the PHI cannot be retrieved.

ARRA

- BREACH NOTIFICATION PROVISIONS:
  - The provisions apply to HIPAA covered entities and their business associates and set forth the requirements for notification to affected individuals, the media, and the Secretary of HHS following a breach of unsecured protected health information.
  - Breach notifications must include the following:
    - A brief description of what happened, including the date of the breach and the date of discovery of the breach, if known

ARRA

- Breach notifications must include the following:
  - A description of the types of unsecured protected health information that were involved in the breach
  - Any steps the individuals should take to protect themselves from potential harm resulting from the breach
  - A brief description of what the covered entity is doing to investigate the breach, to mitigate harm to individuals and to protect against any further breaches.
  - A contact procedure for individuals to ask questions or learn additional information, which must include a toll-free number, an e-mail address, web site or postal address.

ARRA

- Unauthorized Acquisition, Access, Use or Disclosure. "Unauthorized" is an impermissible use or disclosure of protected health information under HIPAA Privacy Rule.
- If you send an email that contains PHI, and that email is intercepted, sent to a wrong address, or printed out and used inappropriately, you may have violated HIPAA and ARRA.

ARRA

- While the state network is secure, it is not encrypted. State employees may use ePass Montana – File Transfer System (FTS) for files that contain PHI. The FTS website can be used by networked DPHHS employees as well as outside entities.
- Here is the link to the FTS. https://transfer.mt.gov/default.aspx
- On the FTS website there are instructions for state employees and outside entities using it for the first time, a "How Do I" tab with questions and answers, and a "Feedback" tab as well as easy to follow links.

HIPAA/ARRA

- IMPORTANT TO REMEMBER:

- ***All*** of DPHHS is considered a covered entity and therefore subject to the rules governed by HIPAA. If you work in the state lab, for Child Support Enforcement, Child and Family Services, at the Montana Veteran's home in Columbia Falls, the Montana State Hospital in Warm Springs, if you work for DPHHS anywhere in Montana, you are part if the covered entity and subject to the HIPAA/ARRA rules.

HIPAA/ARRA

- Risk Assessment – In order to determine whether a covered entity's or business associate's impermissible use or disclosure of PHI constitutes a breach, the covered entity or business associate will need to perform a risk assessment.
  - A risk assessment involves looking at all forms of PHI contained in electronic and paper files held within a covered entity or business associate office locations.

- Risk assessment cont.
  - Covered entities and business associates should consider who impermissibly used or to whom the information was impermissibly disclosed when evaluating the risk of harm to individuals.

  - For example:
  - A covered entity sends out multiple mass mailings. The recipients name and address are at the top of the mailing. The mailing somehow gets off and some people get letters addressed to other people.
    - If a covered entity takes immediate steps to mitigate an impermissible use or disclosure, such as by obtaining the recipients' satisfactory assurances that the information will not be further used or disclosed (through a confidentiality agreement or similar means) or will be destroyed.

- Risk Assessment cont.
  - If such steps eliminate or reduce the risk of harm to the individual to a less than “significant risk”, then we interpret that the security and privacy of the information has not been compromised and, therefore, no breach has occurred.

  - Example two:
  - An impermissible disclosure of PHI is returned prior to it being accessed for an improper purpose.

- Risk assessment cont.
  - A laptop is stolen or lost and then recovered, and a forensic analysis of the computer shows it's information was not opened, altered, transferred, or otherwise compromised, such an incident may not pose a significant risk of harm to the individuals whose information was on the laptop. Therefore, this would not be considered a reportable breach.

- Risk assessment cont.
  - In performing a risk assessment, DPHHS will also consider the type and amount of protected health information involved in the impermissible use or disclosure. If the nature of the PHI does not pose a significant risk of financial, reputational, or other harm, then the violation is not a breach.
  - Example: DPHHS improperly discloses PHI that merely included the name of an individual and the fact that he received services from a hospital, this would constitute a violation of the Privacy Rule, but

- it may not constitute a significant risk of financial or reputational harm to the individual. In contrast, if the information indicates the type of services the individual received (such as oncology services), or that the individual received services from a specialized facility(such as a substance abuse treatment program) or if the PHI includes information that increases the risk of identity theft (such as social security number, account number, or mother's maiden name), then there is a higher likelihood the impermissible use of disclosure compromised the security and privacy of the information.

- A risk assessment will be fact specific and we will keep in mind the many forms of health information, not just information about STD's or mental health, should be considered sensitive for the purpose of the risk of reputational harm – especially in light of fears about employment discrimination.

- Compliance with HIPAA and ARRA regulations is required. If you intentionally or accidentally, send a letter with PHI in it to a wrong person or address, throw in the trash/garbage can a letter containing PHI instead of shredding it, throw away a printed email or even a CD with PHI on/in it, you have made available information (PHI)that is usable, readable, or decipherable to unauthorized individuals. You have potentially violated HIPAA and ARRA regulations. These incidents must be reported and recorded into a database for yearly reporting to the Secretary.

MITIGATION Actions

- If there is a breach of PHI by an employee of DPHHS the following will be expected:
  - 1. The employee will notify their supervisor and or bureau chief.
  - 2. The HIPAA privacy officer will be notified to conduct an investigation and offer mitigation guidelines.
  - 3. All relevant information will be in writing for documentation purposes. This includes:
    - What information was disclosed
    - To whom it was disclosed
    - When it was disclosed
    - When was the disclosure discovered
    - What steps have been taken to date

MITIGATION Actions

- 4. Risk assessment will be conducted
- 5. The incident will be recorded in the HIPAA database by either the HIPAA liaison or the privacy officer.
- 6. If contacted by Office for Civil Rights, or any other investigative authority, all documents will be available to demonstrate DPHHS took action to reduce risk and mitigate any harm.

OFFICE FOR CIVIL RIGHTS

- The Secretary of Health and Human Services has designated the Office for Civil Rights (OCR) as the enforcement agency for HIPAA/ARRA.
- OCR will contact the HIPAA Privacy Officer as well as the individual involved if there is a complaint filed with that individual and agency.
- If you are contacted by OCR, notify your supervisor, Bureau Chief and HIPAA Privacy Officer as soon as possible.

WEB SITES:

- Centers for Medicare and Medicaid – http://www.cms.hhs.gov/HIPAAGenInfo/
- Office for Civil Rights – enforcement of HIPAAhttp://www.hhs.gov/ocr/privacy/
- DPHHS OURS website – training, policies, forms. http://ours.hhs.mt.gov/hipaa/
- Code of Federal Regulations – 45.160 through164 http://www.gpoaccess.gov/cfr/retrieve.html
- Health and Human Services – go to regulations tab http://www.hhs.gov/policies/index.html

- Web sites:
  - File Transfer Service – log in as Montana State Employee
  - https://transfer.mt.gov/default.aspx