This is a basic HIPAA orientation training designed for Plumas County employees who work in covered departments. The focus is on privacy.

What is HIPAA?

- **H**ealth **I**nsurance **P**ortability & **A**ccountability **A**ct
- Federal Law (P.L. 104-191) enacted by Congress & signed by President Clinton in 1996. The compliance deadlines for the different components are different.
- The original intent was to make it easier for people to move from one health insurance plan to another (due to job change, unemployment, change in marital status)

- Major components
  1. Protect patient **privacy** of personal health information (4/03)
  2. Ensure **security** of medical information in all forms (electronic, paper, oral) (4/05)
  3. Set **National Transaction Code Standards** for electronic transmission of health data (10/03)
  4. Use unique **National Identifiers** for employers (7/04), providers(5/07), & health plans on electronic transmissions.

- Objectives
  1. Improve efficiency of health care systems by standardizing electronic codes
  2. Reduce administrative costs
  3. Reduce fraud and abuse
  4. Protect patient privacy, confidentiality and access to their health information

Need for Privacy

Privacy of health information has long been an **ethical obligation** of health care providers. As storage and transmission of information moved to an electronic format, the possibility of unintentional disclosure and intentional misuse increased. **HIPAA** made the ethical obligation to protect the privacy and confidentiality of health information the **law in all states**. HIPAA says **only those with a legitimate or authorized need to know will have access** to protected health information. HIPAA Privacy Rules are preempted by more stringent existing state laws.

What is Private?

Health Information that can be identified to a specific individual is protected (PHI)

Health information means information that is created or received by a County department and relates to the physical or mental health or condition of an individual, the provision of health care to the individual, or payment for health care for the individual.

Individually identifiable means there is a reasonable belief that the information can be used to identify a specific individual. Names, addresses, photos, phone #, drivers license #, social security # make a document individually identifiable. In a small community, general descriptions can be individually identifiable.

Compliance

Compliance is mandatory for Health Plans, Prescription Drug Card Sponsors, Healthcare Clearinghouses, Health Care Providers that transmit standard electronic transactions and many of their Business Associates. In Plumas County, compliance is mandatory for covered departments.

Covered Departments in Plumas County

- Mental Health (provider)
- Public Health Agency (provider)
- Alcohol and Drug (provider)
- Administration (due to relationship w/ covered departments)
- County Counsel (due to relationship w/ covered departments)
- Human Resources (oversees County Health Plan)

Consequences of Failing to Comply

- Loss of revenue – claims not submitted in standard form won't be reimbursed
- Problems with accreditation and licensing
- Harm to clients
- Bad publicity
- Lawsuits
- Fines, penalties and sanctions

Plumas County Personnel Rule 22.10 allows the County to discipline or dismiss any employee who violates HIPAA if they have received County HIPAA training.

The U.S. Department of Health and Human Services will provide technical assistance to obtain voluntary compliance from covered entities but has the authority to use **civil monetary penalties** to enforce HIPAA. **The U.S. Department of Justice** will enforce the **criminal penalties**.

- Civil penalties – $100 per violation, up to $25,000 per year
- Criminal penalties – fines and jail time which increase as the seriousness of the offense increases
  1. Knowingly obtaining or disclosing PHI – $50,000 and/or 1 year
  2. Using false pretenses to access PHI – $100,000 and/or 5 years
  3. Releasing PHI maliciously or selling PHI – $250,000 and/or 10 years

How Does The County Comply?

- Have and follow written policies and procedures
- Appoint Privacy Officer and Security Officer
- Train employees on HIPAA and the Policies and Procedures
- Monitor compliance
- Sanction employees who violate HIPAA Policies and Procedures
- Have Business Associate Agreements with contractors

- Safeguard PHI
- Retain Records the legal length of time
- Mitigate harm caused by improper use or disclosure of PHI

Privacy

- Provide a Notice of Privacy Practices to all clients
- Understand how protections apply
- Understand mandatory and permissible "uses and disclosures"
- Follow the "Minimum Necessary Rule"
- Obtain written Authorization from clients
- Recognize and respect clients' rights and avoid retaliation

Security

- Clarify what is and is not an electronic transmission
- Monitor and control data access

Transaction Code Sets

- Use national standard code when transmitting electronic data for:
  - Health care claims and their status (270,271,837,276,277)
  - Benefit enrollment and maintenance (834)
  - Health care services review (278)
  - Payment and remittance advice (835,820)

How Do Individual Employees Comply?

- Be aware of HIPAA
- Follow the written Policies and Procedures
- Understand how protections apply
- Safeguard PHI
- Understand mandatory and permissible "uses and disclosures"
- Follow the "Minimum Necessary Rule"
- Recognize and respect clients' rights and avoid retaliation
- Report violations

Details of Compliance

Policies and Procedures

- The County has developed HIPAA Privacy policies, procedures and forms. All covered departments have copies and they are also available on the County website.
- Departments with policies **more stringent** than HIPAA may modify the County policies or forms. Written authorization to use the modified documents must be obtained from the County Privacy Officer.
- Security policies and procedures are being developed.

Privacy and Security Officers

- The County Privacy and Security Officer is the CAO.

- The County's provider departments have all designated Privacy Officers or contact people; Stevani Rast for Mental Health, Jocelyn Cote for the Public Health Agency, and Patty Miller for A& D.
- Privacy Officers are responsible for training employees, answering HIPAA related questions that arise during the course of the work day, doing compliance checks, maintaining all records of compliance, and receiving complaints.

Training Employees

- All employees, contract employees, volunteers and interns in covered departments must receive this basic HIPAA training which includes information on whistleblower protections.
- Employees who do client intakes, provide counseling or health care services, or do billing will receive additional training specific to their job.
- Employees will have time to read the policies, procedures and forms and ask questions. Any Privacy Officer may be contacted at any time during the work day to try to answer questions as they arise.
- Plumas County Personnel Rule 22.10 allows the County to discipline or dismiss any employee who violates HIPAA if they have received County HIPAA training **so ask questions if you don't understand something. You will be asked to sign a certification of understanding after this training.**

Monitoring Compliance

- Privacy and Security Officers will monitor compliance but any employee who observes a HIPAA violation or inadvertently makes a HIPAA violation, must bring the problem to the attention of a Privacy or Security Officer.
- Privacy Officers will keep a written report or record of all compliance checks.
- Compliance checks will be done quarterly.

Safeguarding PHI

- Speak with clients in private when possible; move or use a quiet voice if in an area where others may overhear.
- Close the door when speaking on the telephone.
- Never share computer passwords with anyone.
- Documents containing PHI must be kept physically secure from access by unauthorized persons; locked doors, locked file cabinets, locked desks.
- Documents containing PHI must be concealed in an appropriate manner when you are not physically present and labeled confidential before delivery to another department.
- Fax numbers should be checked before sending documents containing PHI

Mitigating Harm

- Employees must report inappropriate or unauthorized use and disclosure so steps can be taken to lessen the potential harm. Appropriate methods of mitigation might include calling an unintended recipient of PHI and telling them to return or destroy the document; informing the person whose PHI was inappropriately used or disclosed of the situation and the steps taken to prevent further disclosure.

Business Associate Agreements

- Must be established with person or entity outside the County organization that provides a service or function that involves the use or disclosure of PHI.
- Provides a clear description of permitted and required uses and disclosures of PHI.
- Requires the Business Associate to protect PHI according to the Privacy Rule and County standards.
- County Departments are not required to monitor Business Associate compliance but must take action if they become aware of a violation of the Business Associate's obligation under the agreement.

Retain Records

- All documents relevant to HIPAA must be retained for 6 years. This includes policies, procedures and forms; training documents and records; Notice of Privacy Practices and acknowledgements; authorizations; requests for access, amendment and restrictions; disclosures; complaints.

Privacy - Notice of Privacy Practices

- Must be **available and posted** in all service delivery sites in the County.
- Must be given to each individual seeking services from County provider or enrolling in County self-insured health plans.
- Staff must document delivery of the NPP with a written acknowledgment of receipt.
- Staff must understand contents of the NPP
    - Describes how the County will handle PHI –obligation to protect and the ways we may use or disclose PHI.
    - Describes individuals rights regarding PHI

Privacy - How Protections Apply

- Use of information
- Disclosure of information
- Requests of information
- Security of information

Privacy – Permissible Uses and Disclosures

- As **authorized** in writing by the individual client or their representative
- For purposes of treatment, payment or health care operations
- As required by law (e.g. court order)
- As detailed in the Notice of Privacy Practices (some require giving individuals the right to agree or object to the use or disclossure)

Privacy – Mandatory Disclosures

- To the U.S. Department of Health and Human Services when it is investigating or reviewing compliance
- To the individual client upon request (exceptions are detailed in County HIPAA Policy PPP16, Individual Rights to Inspect and Copy PHI)

Privacy – Minimum Necessary

- Restricts use, disclosure and requests to the least amount of PHI that is needed to do the job or meet the needs of the request.
- Does not apply to mandatory disclosures; authorized disclosures; uses or disclosures for treatment

Privacy – Authorizations

- May not be combined with a consent for treatment form
- Must be used only for the purpose stated
- Must have an expiration date or event and be signed
- Font must be at least 14
- May be revoked

Privacy – Clients Rights

- Right to receive a copy of the County's Notice of Privacy Practices
- Right to request restrictions on uses and disclosures of PHI
- Right to confidential communications (may specify method of contact)
- Right to inspect and copy PHI
- Right to an accounting of disclosures
- Right to request amendment of PHI
- Right to file complaints without fear of retaliation

Privacy – Avoiding Retaliation
Complaints

- Clients have a right to complain to a County Privacy Officer or to the U.S. Secretary of Health and Human Services at the Office for Civil Rights in San Francisco.
- Complaints must be filed within 180 days of when the complainant knew or should have known that the act complained of occurred.
- Employees, Departments and the County may not penalize, threaten or intimidate individuals in retaliation for filing a complaint.
- Complaints will be logged and investigated. A written report documenting the investigation, conclusions and recommendations will be made.

Reporting Violations / Whistleblowers

- Employees and Business Associates can report suspected violations to Privacy Officers.
- To report suspected violations, an employee **may** need to disclose PHI. Disclosures may **only be made to:** a health oversight agency authorized by law to investigate the conduct or conditions of the County department; an appropriate health care accreditation organization; an attorney retained by the employee for the purpose of determining their legal options with regard to the County's conduct.
- The County may not retaliate against employees or Business Associates who file complaints.

Cooperating with Investigations and Audits

- The County will permit access by the U.S. Secretary of Health and Human Services to facilities, books, records, accounts and other sources of information that are pertinent to a complaint investigation or compliance audit.