Health Insurance Portability and Accountability Act (HIPAA)

General Education
Presented by:
Bureau of Personnel
Department of Health
Department of Human Services
Department of Social Services
Bureau of Information and Telecommunications

Prepared by: Kevin DeWald, Department of Health HIPAA Compliance Officer
HIPAA Education Objectives...

- Understand the HIPAA rule
- Understand penalties for non-compliance
- Understanding of the impact of HIPAA on privacy
- Understand your responsibilities

Prepared by: Kevin DeWald, Department of Health HIPAA Compliance Officer
What is HIPAA...

HIPAA is...
A federal law imposed on all health care organizations, including hospitals, physician offices, home health agencies, nursing homes, and other providers as well as health plans and clearinghouses.
What does HIPAA cover...

- Privacy
  - Compliance date: 04/14/2003

- Transactions and Code Sets
  - Compliance date: 10/16/2003

- Security
  - Compliance date: 04/21/2005
Definitions
HIPAA definitions...

- **Business Associate**
  
  A person or entity that performs a function on behalf of the department, but is not employed by the department.

- **Consumer**
  
  The person or individual who is the subject of protected health information.

- **Covered entity**
  
  A health plan, health care clearinghouse or health care provider who transmits health information in electronic form.

- **Disclosure**
  
  The release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.
HIPAA definitions...

- **Health Care**
  Care, services, or supplies related to the health of an individual. This may include preventive, diagnostic, rehabilitative or other health related services.

- **Protected Health Information (PHI)**
  Individually identifiable information about a consumer’s health related condition or case in oral, written or electronic format.

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

- **Workforce**
  Employees, volunteers, trainees, interns, and other persons whose conduct is under the direct control of a covered entity.
Transactions & Code Sets
Transactions...

- The final rule adopts national standards for transactions in electronic format. These were developed by the American National Standards Institute (ANSI).
Transactions...

The ANSI standards adopted under the final Rule include:

- 837 Health Care Claim (Professional, Institutional, and Dental)
- 270/271 Health Care Eligibility Benefit Inquiry and Response
- 278 Health Care Services Request for Review and Response
- 276/277 Health Care Claim Status Request and Response
- 834 Benefit Enrollment and Maintenance
- 835 Health Care Claim Payment/Remittance Advice
- 820 Health Plan Premium Payments

Prepared by: Kevin DeWald, Department of Health HIPAA Compliance Officer
When conducting one of the electronic transactions covered entities must use the applicable medical data code sets.

- CPT-4 (physician services)
- CDT-3 (dental services)
- ICD9-CM (diseases, impairments, causes of injury and disease, inpatient hospital services procedure codes)
- HCPCS Level II (equipment, supplies and other health-related services)
- NDC (drugs dispensed by retail pharmacies)
Privacy
Privacy...

- Under the privacy rule, health plans, health care clearinghouses and health care providers must guard against misuse of individuals’ identifiable health information. The privacy rule creates a floor of national protection for the privacy of consumers most sensitive information – health information.

Prepared by: Kevin DeWald, Department of Health HIPAA Compliance Officer
What is confidential...

- Any information about a consumer in written, oral or electronic format is considered protected health information (PHI).

What does this include...
- Name
- Address
- Age
- Social security number
- Phone number
- E-mail address
- Diagnosis
- Medical history
- Medications
- Medical record numbers
- And more....
What does the Privacy rule say about using my computer...

- Keep your passwords secret
- Do not log into your computer using someone else’s password
- Turn computer screens away from public view when possible. Implement screen savers when the monitor cannot be turned from view.

More information on Security will be available when the Security Rule goes into effect on 04/21/2005.

Prepared by: Kevin DeWald, Department of Health HIPAA Compliance Officer
Enforcing the rule...

Penalties for breaking the privacy rule

- **Criminal penalties under HIPAA:**
  - Maximum of 10 years in jail and a $250,000 fine for serious offenses

- **Civil penalties under HIPAA:**
  - Maximum fine of $25,000 per violation

- **Organizational actions:**
  - Employee disciplinary actions including suspension or termination for serious violations of the department’s policies and procedures.
Each department impacted by HIPAA will have a privacy or compliance officer who will:

- Manage and develop department standards, policies and procedures
- Oversee education and training of the workforce
- Enforce the policies and procedures
- Investigate complaints and violations

Prepared by: Kevin DeWald, Department of Health HIPAA Compliance Officer
State of South Dakota Agencies with Privacy officers are...

- Department of Health
- Department of Human Services
- Department of Social Services
- Bureau of Information and Telecommunications
Confidentiality Agreement
At the end of this HIPAA general education, employees of certain departments may be asked to sign a confidentiality agreement. By signing you agree to:

- Use confidential information only in performing your duties
- Dispose of protected health information properly
- Follow the department’s policies and procedures

Prepared by: Kevin DeWald, Department of Health HIPAA Compliance Officer
Privacy Rule Provisions
Notice of Privacy Practices...

- Provides the consumer with a notice of the way the department uses and shares their health information
- Explains to the consumer their right to confidentiality and access to his/her information
- Must be posted prominently in the department or office for easy view by consumers

Prepared by: Kevin DeWald, Department of Health HIPAA Compliance Officer
How Protected Health Information (PHI) may be used...

- **Treatment**
  - PHI may be used or disclosed to provide, coordinate, or manage consumer’s health care and related services.

- **Payment**
  - PHI may be used or disclosed to obtain payment for the health care services consumers receive.

- **Health Care Operations**
  - PHI may be used or disclosed in order to manage our department programs and activities.

- **Required by Law**
  - PHI may be used or disclosed when required by federal or state law.
How PHI may be used...

- **Required for Law Enforcement**
  - PHI may be used or disclosed when required by court order, subpoena, warrant, summons, or similar legal process.

- **Public Health Activities**
  - PHI may be used or disclosed for public health activities such as vital statistics (births, deaths, etc.) or disease control.

- **Public Health Oversight Activities**
  - PHI may be used or disclosed for public health oversight activities, such as inspecting health care providers.

- **Abuse Reports and Investigations**
  - PHI may be used or disclosed as required by law to receive and investigate reports of abuse.
How PHI may be used...

- Avert a Serious Threat to Health or Safety
  - PHI may be used or disclosed when necessary to prevent a serious threat to the health or safety of the consumer or other individuals.

- Research
  - PHI may be used or disclosed for research studies and to develop research reports.

- Appointments
  - PHI may be used or disclosed to send reminders for health care appointments.
Consumer rights under the Privacy Rule
Right to access...

- A consumer has the right to inspect and/or obtain a copy of his/her protected health information held by the department.
A consumer has the right to request amendments to his/her protected health information. Departments are not required to automatically make the changes the consumer requests.
Right to an accounting of disclosures...

- A consumer has the right to request an accounting of the disclosures of his/her PHI. These requests may be suspended for certain reasons authorized by law.
Right to request restrictions...

- A consumer may ask that PHI not be used or disclosed for treatment, payment, or health care operations. These requests may be denied for certain reasons authorized by law.
Right to request confidential communications...

- A consumer may request that communications with them remain confidential. This may be done through contact at an alternate phone number, address or e-mail. All reasonable requests must be accommodated.
Right to file a complaint...

A consumer who feels their rights under the privacy rule have been violated may file a formal complaint with the department Compliance Officer, or with the Secretary of the U.S. Department of Health and Human Services. No retaliation will occur against the participant filing a complaint.
Other Standards under the Privacy Rule
Other standards...

- **Business Associates**
  - A person or entity that performs a function on behalf of the department, but is not employed by the department. A Business Associate Contract assures that PHI they use or disclose will remain confidential.

- **De-Identification**
  - Gives standards to assure PHI that is released cannot be used to identify the individual.

- **Limited Data Set**
  - Lists the data which must be removed to be considered de-identified.

- **Marketing**
  - Making communication about a product or service a purpose of which is to encourage recipients of the communication to purchase or use the product or service
Other standards...

- **Minimum Necessary**
  - Assures that the minimum amount of information will be used to complete the job or task.

- **Research**
  - A systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

Prepared by: Kevin DeWald, Department of Health HIPAA Compliance Officer
Security Rule
The proposed security rule addresses the following areas:

- Administrative procedures
- Physical safeguards
- Technical data security services
- Technical security mechanisms

Compliance Date

04/21/2005
Cases to consider
Case #1…

Your sister’s close friend is receiving services from the department where you work. Your sister asks you to find out what you can about her friend’s case. Should you look up the friend’s medical information to give to your sister?

**NO** – Even if you and your sister have the best intentions, you do not have the right to access PHI about her friend’s case. You should not seek out PHI unless you need it to do your job. When you happen to hear confidential information, do not repeat it to anyone.
Case #2

You are walking by a trashcan and notice a pile of photocopied records containing PHI has been laid on top of the trash. How should you handle this?

Don’t just take the records to be shredded. Gather the records and take them to your supervisor. He or she will report it to the department Compliance Officer, and they will determine why the records were not disposed of properly.
You pass by the roster of individuals being seen today in your department. You spot the name of a close friend. Should you stop by and say hello?

No - If you learned of your friend’s appointment by looking at the roster, you should not stop by unless your job responsibilities take you there.

If your job responsibilities do not take you there, but the individual or their family member has told you they are going to be there, you may then stop by.
Case #4

- A co-worker is having trouble logging in to the department’s information system. They ask for your login name and password so they can try them. Should you share that information with them?

**NO** – The HIPAA security standards require the use of individual passwords for each member of the workforce. If you let others use your password, you may be held responsible if your co-worker gains access to information inappropriately. You should keep your login and passwords secure.

Prepared by: Kevin DeWald, Department of Health HIPAA Compliance Officer
Test your knowledge
Question #1...

When are you free to repeat protected health information that you hear while on the job?

a. After you no longer work for the department
b. After the consumer dies
c. Only if you know the consumer won’t mind
d. Only when necessary to do your job
Answer...

D

Only when needed to perform your job are you allowed to release PHI that you learn while at work.
Question #2...

You see an open recycling bin full of paper. You can see names, addresses, and diagnoses on them. What should you do?

a. Nothing
b. Show it to your supervisor or your department’s Compliance Officer so they can determine why it was put there
c. Read the report and try to figure out who disposed of it improperly
d. None of the above
Your department Compliance Officer or Privacy Officer should be notified so that they may find the source. They will want to ensure documents that contain PHI are disposed of properly.
Question #3...

What question should you ask yourself before looking at a consumer’s information?

a. Would the consumer mind if I looked at this?
b. Do I need to know this to do my job?
c. Can anyone see what I’m doing?
d. All of the above
While performing your job duties, you may need access to a consumer’s PHI. You should remember that you only need the information related to performance of that duty.
Question #4...

Which of the following is NOT a common practice to protect the confidentiality of consumer’s information?

a. Keeping computers logged out of the information system when not in use
b. Storing paper records in locked file cabinets or rooms
c. Throwing paper containing PHI in the trash can
d. Pointing computer screens away from the public when possible

Prepared by: Kevin DeWald, Department of Health HIPAA Compliance Officer
C

Documents that contain PHI should be disposed of properly, by shredding or placing in a secure area for recycling.
Question #5…

Under what circumstances is it acceptable to share your password?

a. When your co-worker forgets his/her password
b. When it saves time to use a common password
c. When you know you can trust the person to use it wisely
d. Never
Answer...

D

- You should always keep your passwords private. Remember that if someone uses your password you may be held responsible for inappropriate use by the other party.
Question #6...

Which of the following is considered protected health information under HIPAA?

a. The consumer’s address
b. The consumer’s medical record number
c. The consumer’s phone number
d. All of the above
D

These items and others are considered PHI. Check with your supervisor or your department’s Compliance Officer for more information.
Question #7...

Which of the following types of information does HIPAA’s privacy rule protect?

a. Consumer information in electronic form
b. Consumer information communicated orally
c. Consumer information in paper form
d. All of the above
The HIPAA privacy rule protects information used or disclosed in electronic or written format. Oral communications are protected under the HIPAA privacy regulation.
Question #8...

Which of the following is a duty of the Compliance Official?

a. Develop the department’s privacy standards, policies, and procedures
b. Oversee education and training of workforce
c. Enforce the rules and investigate violations
d. All of the above
The Compliance Officer or Privacy Officer has many responsibilities in addition to those included on this list. You may wish to view your department’s job description for the Compliance Officer for more information.
Question #9...

What should you do if a consumer complains about their rights being violated under the privacy rule?

a. Notify your department’s Compliance Official who is responsible for handling complaints
b. Ask the program participant not tell anyone
c. Nothing – It’s not your job to handle complaints
d. None of the above
Answer...

A

- The Compliance Officer if responsible for investigating any complaint filed by a consumer.
Question #10...

What type of rule is HIPAA?

a. A state law imposed on clinics only
b. A federal law imposed on all health care providers, health plans and clearinghouses
c. A guide set forth by the South Dakota Department of Health
d. A local law
B

- HIPAA is a federal law that all health care providers, clearinghouses and health plans must follow. The HIPAA regulation is published in the Federal Register.

Prepared by: Kevin DeWald, Department of Health HIPAA Compliance Officer
Questions...

Please contact your supervisor or department’s Compliance Officer if you have any questions.
Thank you!

Bureau of Personnel
Department of Health
Department of Human Services
Department of Social Services
Bureau of Information and Telecommunications

Please follow instructions on the next page to complete your General Education session.

Prepared by: Kevin DeWald, Department of Health HIPAA Compliance Officer
To complete your HIPAA General Education session, please click on the link below to submit and print the HIPAA form. Please forward this form to your supervisor.

By clicking this link, you acknowledge that you have reviewed the HIPAA General Education presentation.

http://intranet.bop.sd.gov/hipaa/pr48hipaa.aspx