HIPAA PRIVACY POLICIES & PROCEDURES

Department of Behavioral Health and Developmental Services
DBHHDS

GENERAL AWARENESS TRAINING

March 2012

HIPAA Humor (North Dakota Dept of Health)

- HIPAA-Ectomy - the removal of individual identifiable health information from records
- HIPAA-Glycemia – a low level of understanding of the HIPAA regulations
- HIPAA-Phobia – a morbid fear of HIPAA regulations
- HIPAA-Thermia – the unexplained chill that is running down the back of anyone associated with HIPAA

Please Note:

- This summary/overview is not intended to be comprehensive.
- You must:
  - Review our complete policies & procedures referenced later within this presentation;
  - Consult with the agency's privacy officer for guidance/clarification on specific HIPAA-related issues.
- When in doubt – ASK!

Federal Health Information Privacy & Security Provisions include:

- Privacy Rules – effective since April 14, 2003, to:
  - Keep protected health information (PHI) confidential, and
  - Discipline individuals who fail to keep patient information confidential
- Security Rules – effective since April 21, 2005, to:
  - Ensure the confidentiality, integrity, and availability of all electronic protected health information, and
  - Ensure compliance by the workforce

Privacy & Virginia Laws

- In addition to federal laws, the Code of Virginia also addresses health privacy laws.
  - Many provisions are found in sections 32.1-127.1:03 and 32.7-121.1:04.
  - There are also other Code sections that may impact health information privacy in specific circumstances.
  - The Virginia Human Rights regulations also include privacy protections for individual health information.
  - The Office of the Attorney General works with the Privacy Officer to clarify when federal preemptions may apply, and when state laws provide more stringent privacy protections.

Goals of HIPAA

- Strike a balance between government interest in health information and individual rights to maintain control
- Allow individuals more control over their personal health information
- Impose accountability for breaches of confidentiality or security
- Set boundaries for providers regarding patient's privacy and confidentiality
- Require safeguards to protect against reasonably anticipated unauthorized uses or disclosures of health information
- Encourage use of electronic record-keeping systems for health data, while protecting against reasonably anticipated threats or hazards to the security or integrity of the information

Privacy & Security Rules Are Necessary because…

- **Look at some recent headlines:**
  - "Identity Theft is America's fastest growing crime"
  - "Hospital fires employees for leaking VIP info to media"
  - "Hackers steal tens of thousands of ID numbers from popular websites…"
  - "Contract employees accused of stealing PHI"
  - "Personal info being collected and sold (using telephone numbers)"
  - "Internet connects sperm donors with offspring."

Privacy & Security Officials

- Denise A. Dunn – Chief Privacy Officer
  - Central Office Room 1134
  - 804-371-2181
- John Willinger – Department Acting Security Officer
  - Central Office Room 511
  - 804-786-4143

All Staff Must Review the DBHDS Privacy Provisions

- Our Privacy, Policies & Procedures for the Use and Disclosure of Protected Health Information …
  - consist of ten subject-specific chapters with more detailed requirements for workforce compliance with HIPAA and related confidentiality rules & regulations
  - Go to CODIE, click on *Instructions and Policies*
  - Scroll to and click on *DI 1001 (PHI)03*

Safeguarding Private Information Is Everyone's Responsibility at DBHDS

- If you have access to any patient or personal information in any format, you are responsible for keeping it safe and confidential.
- There are consequences for individuals who violate privacy of security regulations.
- Consequences may include disciplinary actions as well as civil and criminal penalties.

Bottom Line – Privacy is Just Good Customer Service

- Keeping each individual's best interests first,
- While striving to preserve their privacy rights.

- … and then it's good Record Management:
  - Keeping records accessible, but safe and secure at the same time, while
  - Preserving the integrity of each record.

How Do Individuals Know What Their Privacy Rights Are?

- The DBHDS **Notice of Privacy Practices** must be given to each individual upon admission into our system. It is posted on our website, and tells them how:
  - PHI may be **used or disclosed** by the care provider
  - To **access** their personal medical records
  - To request to **correct** their records if they appear incorrect
  - To request **alternative communications** of their medical information that are more confidential
  - To request **restrictions** on release of personal health information
  - To request an **accounting** of certain disclosures of personal health information
  - To **object** to certain disclosures of personal health information

Let's Think About It…

Mrs. Brown calls her husband's physician and asks for his lab test results. She says that Mr. Brown is at work and asked her to call. The test results are positive for a sexually transmitted disease. The physician declines to give the results to Mrs. Brown and asks her to get her husband to call personally for the lab results. Mrs. Brown is irate and states "HIPAA laws say you can share health information with a family member." Who is right in this case?

- Mrs. Brown
- The Physician

The Physician

So What Is PHI?

- PHI (Protected Health Information) = any health information that links an identifiable person with his or her health condition.
  - Some identifiers include:
    - Names
    - Dates
    - Numbers
    - Addresses
    - Graphics
- Every identifier listed in the HIPAA regulations is outlined in DI 1001 (PHI)03

PHI Comes In All Kinds of Formats

- Paper or “hard-copy”: records, labels, correspondence
- Electronic: computerized, digitized, video, audio
- Communications: verbal, sign language, etc.

If all the identifiers are removed, the information is no longer PHI…

- It is **de-identified**

General Rule Regarding PHI

PHI may not be used or disclosed except as permitted or required by law

Required PHI Disclosures …

- To the individual who is the subject of the PHI – when requested
- When required by the Secretary of Health and Human Services

Permitted PHI Disclosures …

- To the individual who is the subject of the PHI
- For treatment, payment and healthcare operations (**TPO**) as defined by the HIPAA regulations
- As otherwise **permitted** or **agreed** (in keeping with HIPAA regulations)
- As **AUTHORIZED** by the individual or their legal representative

Treatment Defined (45 CFR 164.506)

- The provision, coordination, or management of health care and related services among health care providers or by a health care provider and a third party, consultation between health care providers regarding a patient, or the referral of a patient from one health care provider to another

Payment Defined (45 CFR 164.501)

- The various activities of health care providers to obtain payment or be reimbursed for their services…

Health care operations (45 CFR 164.501)

- Certain administrative, financial, legal, and quality improvement activities of a covered entity that are necessary to run its business and to support the core functions of treatment and payment…

PHI Uses & Disclosures – When No Authorization Required …

- Uses & disclosures required by law
- Uses & disclosures for public health activities
- Disclosures about victims of abuse, neglect, or domestic violence to law enforcement and other appropriate authorities & officials
- Uses & disclosures for legally authorized health oversight activities

PHI Uses & Disclosures – When No Authorization Required …

- Disclosures for Judicial and Administrative Proceedings
  - Court orders
  - Subpoenas
- Disclosures for law enforcement purposes

PHI Uses & Disclosures – When No Authorization Required …

- Uses & disclosures about decedents
  - Coroners, medical examiners, funeral directors
- Uses & disclosures for organ donation purposes
- Uses & Disclosures for certain research purposes

PHI Uses & Disclosures – When No Authorization Required

- Uses & disclosures to avert a serious threat to health or safety
- Uses & disclosures for specialized government functions (i.e. coordination of agency benefits for same or similar populations)
- Disclosures for workers' compensation purposes

Uses & Disclosures When Authorization IS REQUIRED…

- For all uses and disclosures not expressly permitted, or not expressly identified as requiring no authorization

Minimum Necessary Rule

- When using, disclosing or requesting PHI..
  - We must make reasonable efforts to limit PHI to the **minimum necessary** to accomplish the intended purpose of the use, disclosure or request

When Minimum Necessary Rule Does **NOT** Apply …

- Disclosure to or requests by providers **for treatment**
- Uses or disclosures made to the **individual**
- Uses or disclosures made pursuant to an **authorization**

When Minimum Necessary Rule Does NOT Apply …

- Disclosures to the Secretary of Health and Human Services
- Uses or disclosures required by law
- Uses or disclosures required for compliance with HIPAA

Business Associate Agreements

- Who Is A Business Associate?
  - A person who
    - On behalf of DBHDS performs or assists in
      - A function or activity involving the use or disclosure of PHI
      - This includes claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing, or …

Who Is A Business Associate? (cont'd)

- … any other function or activity regulated by HIPAA provisions; or that
  - provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for DBHDS where the provisions of the service involve the disclosure of PHI

Business Associates (cont'd)

- We may disclose PHI to a business associate if we first receive satisfactory assurances that the business associate will appropriately safeguard the information.
- Satisfactory assurances require:
  - Business Associate Contract, or
  - Memorandum of Understanding

Business Associates (cont'd)

- HITECH Act (Health Information Technology for Economic and Clinical Health Act) Changes regarding Business Associates:
- For the first time, business associates must comply directly with many of HIPAA's Security Rules, which require:

Business Associates (cont'd)

- Appointing a security officer,
- Developing written policies and procedures,
- Training the workforce on how to protect electronic protected health information ("EPHI")

Business Associates (cont'd)

- Business associates also will need to follow HIPAA's Security Rules relating to:
- Physical safeguards
- Technical safeguards
- Adoption of written policies and procedures

Failure to do so will subject a business associate to civil monetary penalties and criminal penalties.

Privacy Violations Consequences

- HIPAA Privacy Rules are enforced by the Office of Civil Rights (OCR)
- Violations can result in personal liability, either civil or criminal sanctions, including fines, jail time or both
- DBHDS sanctions may include disciplinary actions or termination

Let's Review…

- Individual Health Information is considered de-identified if data such as names and social security numbers are removed, but other information such as dates of service and zip codes do not have to be removed.
  - True
  - False

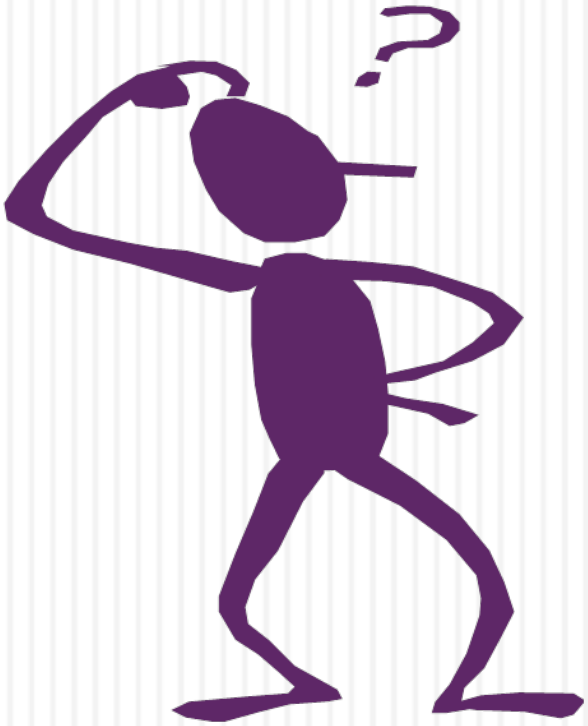
- False

Let's Think About It…

- A drug company wants to send information about a new drug to individuals with a certain diagnosis. They ask one of our facilities or Central Office units for a list of names and addresses of these persons. We do not need to get authorization to release this information.
  - True
  - False

- False

Speaking of Confidentiality



How Much Is Enough? How Much Is Too Much?

Three Types of Problem Disclosures…

- Incidental
- Accidental
- Intentional

Incidental Disclosures

- If you are taking **reasonable precautions** to safeguard an individual's health information, and someone happens to hear or see PHI that you are using, you are not necessarily responsible for that type of disclosure.

Reasonable Precautions to Avoid Incidental Disclosures …

- Speak in as low a voice as possible
- Move to as private an area as possible within the circumstances at hand
- Ask individuals if they are comfortable with the setting (and offer alternatives if possible)
- Cover documents and shield computer screens in public areas to make them as secure as possible

Examples of Incidental Disclosures

A visitor or someone else sees or hears while you are…

- **Reviewing records & orally coordinating services at an assessment station or appointment desk**
- Viewing and discussing lab results, satisfaction survey results, or a personal complaint with an individual or other provider in a shared working space
- **Discussing an individual's condition or treatment with him or her, or with family in a semi-private room**
- Discussing an individual's condition with students or other trainees during rounds in an academic institution or other training setting

Each of these situations still require you to take **reasonable precautions!**

Accidental Disclosures

- **Mistakes Happen** … If you disclose private data in error to an unauthorized person …
  - Acknowledge the mistake, notify your supervisor or Privacy Officer immediately
  - Learn from the error --- change procedures or practices as needed
  - Assist in correcting or recovering from the error ONLY if instructed to do so – **don't try to cover it up** or "make it right" on your own.

Immediately report Accidental disclosures to Privacy Officer!

Intentional Disclosures

- If you **ignore the rules** and carelessly or deliberately use or disclose protected health information inappropriately, you can expect the possibility of:
  - Disciplinary action
  - Civil liability
  - Criminal charges

Intentional Violations: Examples

- **Improper Use of Passwords** can become Intentional Violations
  - Sharing, posting or distributing personal password or account access information
  - Allowing co-workers to use your login
  - Knowledge of unauthorized use of passwords by co-workers, and failure to report
  - Attempting to acquire or use another person's access information or authorization

Intentional Violations: More Examples

- **Improper use of Computers** can become Intentional Security Violations
  - Failing to secure your workstation which contains PHI
  - Emailing PHI outside of the DBHDS network system
  - Posting PHI on the Internet without authorization, or with inadequate security measures

Intentional Violations: Even More Examples

- Accessing PHI outside of your "professional need to know" capacity - either from personal curiosity or as a favor for someone else
- Accessing PHI at home and leaving it visible to other relatives, friends, roommates, etc.
- Selling or inappropriately releasing PHI to the media
- Discussing PHI in public hallways, elevators, etc. without taking reasonable precautions

When To Report Violations

- **All Accidental and Intentional violations, *known and suspected*, must be reported immediately…**
  - **So they can be investigated and managed**
  - **So they can be prevented from happening again**
  - **So damages can be kept to a minimum**
  - **To minimize your personal risk**
- **Incidental disclosures do not need to be reported to the Privacy Office – but if you're not sure, report anyway!**

Let's Review…

- You're walking in the hallway behind a staff member who is talking on his cell phone. You can clearly hear his conversation, which includes references to several individuals receiving treatment in our system … names, locations, and conditions. At one point he says, "you won't believe who was referred here for treatment …"
- Are you required to report this as a privacy breach?
  - Yes
  - No

- Yes

Administrative Safeguards Available to You:

- **Policies & Procedures** - about using & disclosing electronic data, and assigning responsibilities for securing e-data, including PHI, during disasters
- **Privacy & Security Officers**- to consult for policy interpretations and to manage complaints & incidents
- **Education & Training** - to inform all workforce members of the privacy and security rules
- **Internal Audit Tools** -to determine routine compliance with privacy & security rules and regulations

Physical Safeguards

- **Identification**
  - All staff, visitors, volunteers, etc. should display approved ID badges in all areas where PHI documents are accessible
- **Locks, Doors and other Barriers**
  - Lock offices, workspaces, treatment areas, labs, conference rooms, storage rooms, etc. where there are PHI documents
- **Document Covers**
  - Protect all paper documents containing PHI in folders, binders, etc.
  - Transport documents with PHI in a manner to avoid inappropriate disclosures

PHI in E-Mails

- **Individual to Care Provider:** If an individual who is receiving, has received, or is seeking services within our system wishes to exchange email messages with you…
  - Inform him or her of the risks for accidental and unauthorized disclosures when using email
  - You can receive emails from these individuals, but never use PHI in emails to them without written authorization
- **Provider/Staff to Provider/Staff**
  - Use emails **only** within the DBHDS network system

PHI Disposal

- Disposing of document or other formats containing PHI -
  - **Preferred Method:** Shred, deface, etc. or destroy immediately
  - **Next Best:** Place in secure container in secure place
- Follow DBHDS policies for destruction of records
  - All records must be retained or destroyed in accordance with HIPAA regulations and Library of Virginia guidelines

Think Fast

Your coworker has forgotten his password and needs to enter some critical data in the system before going home, so you let him use your log-on and password

While in the system, he looks up some personal identification information about another co-worker. Later, that co-worker complains that she suspects someone has accessed her PHI. If an audit is performed, who will be responsible for the authorized access?

___ My friend ___ I will ___ Both of us

___ No one, it was work-related

- I will

HIP HIPAA HOORAY!!!

You have successfully completed the HIPAA Privacy Awareness Training!

- There may be lots more information you need to know based on your job responsibilities.
- Review your EWP with your supervisor for further guidance and be certain to understand the PHI Access Level assigned to you.
- Consult with the privacy officer as you proceed on projects impacted by HIPAA.
- Again,
  - **If in doubt….. ASK!!!!**

University of Florida HIPAA Privacy Awareness Training

Some portions of this this presentation were adapted from the University of Florida HIPAA Privacy Awareness Training

- http://privacy.health.ufl.edu/training/hipaaPrivacy/instructions.shtml