Overview of the Health Insurance Portability and Accountability Act (HIPAA)

And 42 CFR Part 2

More than just HIPAA

- 42 CFR Part 2
- Code of Virginia – VDSS programs
- FTC Health Breach Notification Rule
- Title 21 of the Code of Federal Regulations (21 CFR Part 11)
- Privacy Act of 1974
- Family Educational Rights and Privacy Act (FERPA)
- Payment Card Industry Data Security Standard (PCI DSS)
- Violence Against Women Act
- State Breach Notification, Social Security Numbers, Data Protection, and MANY other laws

Revised - 03/2015

Purpose of HIPAA

Initial Impact: Improve portability and continuity of health insurance coverage.

Longer term goals:

- To combat waste, fraud, and abuse in health insurance and health care delivery
- To simplify the **administration** of health insurance by:
  - Standardizing the interchange of electronic data for specified administrative and financial transactions; and
  - Protecting the security, confidentiality, integrity, and availability of any protected health information

Revised - 03/2015

Purpose of HIPAA Continued

Protect the Rights of individuals, including:

- ***Right*** to access their own health care information
- ***Right*** to request an amendment or correction of protected health information that is inaccurate or incomplete
- ***Right*** to request restriction of uses and disclosures
- ***Right*** to receive accounting of when information had been disclosed for purposes other than treatment, payment and health care operations
- ***Right*** to receive written notice of information practices from health plans and providers
- ***Right*** to challenge the covered entity's use of disclosure of PHI through complaints to the Privacy Officer and through the Secretary of Human Services

Revised - 03/2015

Why Comply with HIPAA?

- **Required by Federal law - April 14, 2003, revised April 21, 2005 (non-compliance imposes severe penalties)**
- Decreases any Public Relations Risk Issues
- Avoids denied and/or delayed reimbursements when claims are submitted in the required standard format
- Minimizes Potential Risks:
  1. Non-Accreditation by national accreditation agencies such as, Joint Commission on Accreditation of Health Care Organizations (JCAHO)
  2. Business risk from lawsuits & criminal penalties.
- Reduces long term health care costs

Revised - 03/2015

HIPAA Penalties & Enforcement - HITECH

- **Health Information Technology for Economic and Clinical Health (HITECH) Act**
  - addresses the privacy and security concerns associated with the electronic transmission of health information, in part, through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules
- **Enforcement has been delegated to the Office for Civil Rights (OCR) for civil enforcement and Department of Justice (DOJ) for criminal enforcement**

Revised - 03/2015

HIPAA--Key Terms

- Covered Entity (CE)
- Hybrid Entity (HE)
- Business Associates (BA)
- Protected Health Information (PHI)
- Privacy
- Security
- Electronic Transactions

Revised - 03/2015

HIPAA--Key Terms

- Minimum Necessary
- Reasonable Safeguards
- Uses & Disclosures
- Consent
- Authorizations
- Notice of Privacy Practices

Revised - 03/2015

HIPAA Key Terms – Covered Entity

- ***Covered Entities*** **are health plans, clearinghouses and/or health care providers that are businesses that must comply with HIPAA regulations**
- **Examples of Covered Entities include:**
  1. **Health plans – Kaiser, BCBS, Medicare, Medicaid**
  2. **Health care clearinghouses – businesses that route electronic data between payers & providers (e.g., billing services such as Cerner)**
  3. **Health care providers who transmit PHI in electronic format in connection with a HIPAA transaction (e.g., hospitals, independently licensed practitioners, Public Health Departments, Home Health)**

Revised - 03/2015

HIPAA Key Terms – Covered Entity Functions

- Activities of a *Covered Entity* that relate to covered functions under HIPAA regulations include:
  - Quality assessment and improvement/outcome evaluations
  - Review competence or qualifications of professionals
  - Training, accreditation, certification, licensing
  - Underwriting, premium rating, etc.
  - Medical review, audit, compliance
  - General administrative activities
  - Customer service, due diligence, internal grievances

Revised - 03/2015

HIPAA Key Terms – Business Associates

- *Business Associates* are persons and/or businesses performing services for or on behalf of the covered entity and **requires** a written contract or interagency agreement
  - For example: DHS contracts for medical services with profit or non-profit businesses, e.g., laboratories, group homes, support services
  - Maintain a "Chain of Trust" agreement to exchange data and protect its integrity and confidentiality

Note: Excludes persons who are part of the Covered Entity's workforce (e.g., employees, physicians with staff privileges, other contractors).

Revised - 03/2015

HIPAA Key Terms - Protected Health Information (PHI)

***Protected Health Information* (PHI) Definition**

- Relates to a person's past, present or future physical or mental health, the provision of health care, or the payment of health care;
- Identifies, or could be used to identify the person who is the subject of the information

Code of Virginia Definition:

- Any data of which the compromise with respect to ***confidentiality, integrity, and/or availability could have a material adverse effect on COV interests, the conduct of Agency programs, or the privacy to which individuals are entitled***

Revised - 03/2015

Commonly Used HIPAA Terms

- ***Minimum Necessary*** **– Least amount of information disclosed, used, or requested**
- ***Reasonable Safeguards*** **– The use of administrative, technical and physical safeguards to limit the incidental uses and disclosures of PHI**
- ***Uses & Disclosures*** **– May only use/disclose PHI for the following reasons:**
  - **Treatment, payment and operations**
  - **With individual's permission**
  - **To the individual**

Revised - 03/2015

Commonly Used HIPAA Terms

Consent **– Allows and organization to use PHI for its own purposes, i.e. treatment, data bases. Consents do not waive the requirement for authorizations.**

Authorizations **– Refers to the permission an individual grants to the covered entity to disclose information; authorization must be obtained prior to disclosing any PHI.**

Notice of Privacy Practices **– Document that notifies an individual of its privacy practices, including uses and disclosures.** ***(The signature page must be signed and dated by the individual and staff member.)***

Revised - 03/2015

What Information is Protected?

- PHI may be any information created on behalf of an individual or received by a covered entity from a third party; this includes information that is oral or recorded, and is transmitted or maintained in ***any*** form or medium
- **Includes demographics & photographs**
- *Disclosure of PHI is prohibited without authorization of the individual receiving services or explicitly permitted or required by the regulation*

Revised - 03/2015

What Information is Individually Identifiable?

- **Name**
- **Driver's license number**
- **Phone or fax number**
- **ID or account number**
- **Some biometric identifier (finger or voice print)**
- **Social security number**
- **Address (either street or e-mail)**
- **Health plan ID number**
- **Photograph or likeness**
- **Family members/Friends**
- **Social media, e.g. Facebook, Twitter, etc.**

These elements are considered Protected Health Information--PHI

Revised - 03/2015

Exemptions on Disclosure of PHI

***Disclosures of PHI are required by law*:**

- **Public Health reporting (communicable diseases, etc.)**
- **Abuse or neglect situations**
- **Suicidal/homicidal intent**
- **Judicial and Administrative Proceedings (court order, etc.)**
- **To comply with worker compensation laws**
- **Law Enforcement Purposes (as required)**
- **Other Government and Military**
- **Organ donor purposes relating to a cadaver**

OCR Statement on January 15, 2013 - *reminder that confidentiality laws do not interfere with our duty to warn/mandated reporting*

Revised - 03/2015

Violence Against Women Act

"The Violence Against Women Act (VAWA) is a landmark piece of legislation that sought to improve criminal justice and community-based responses to domestic violence, dating violence, sexual assault and stalking in the United States."
(*http://www.thehotline.org*)

HIPAA & VAWA Confidentiality
(http://tools.nnedv.org/faq/faq-flc/flc-hippa)

Revised - 03/2015

Violence Against Women Act (cont'd)

REMEMBER:

- Enter as little information as possible about the victim
- Avoid using email to transmit the victim's information
- Be vigilant to protect the victim's location

Contact:

- Jo Johnson, Project Coordinator ext. 1678
- Maurice Hendrix, ext. 1513
- Project PEACE
  (http://www.arlingtonva.us/departments/HumanServices/ChildrenFamily/page58498.aspx)

Revised - 03/2015

42 CFR

Prohibits disclosure of any substance abuse-related information within the individual's medical record to individual's external to the substance abuse or co-occurring treatment program without specific individual's authorization

- 42 CFR – cannot identify the individual's status or SA diagnosis
- 42 CFR - more restrictive than HIPAA

Revised - 03/2015

42 CFR

Exemptions:

- Medical emergency – minimal necessary
- Subpoena and a specific authorizing court order - all responses are facilitated by the DHS Privacy Officer and County Attorney staff

Revised - 03/2015

Minimum Necessary Exercise

- Johnny is a 15 year old individual diagnosed with major depression and substance dependence. He was recently removed from his home and is now in a residential treatment program. Johnny's biological mother and father are receiving mental health and financial assistance services from DHS. Johnny has an appointment with Dr. Martins today at 4.

Revised - 03/2015

Minimum Necessary – Front Desk

-

Johnny has an appointment with Dr. Martins today at 4.

Revised - 03/2015

Minimum Necessary - Billing

- Johnny is a 15 year old individual diagnosed with major depression and substance dependence.

Johnny has an appointment with Dr. Martins today at 4.

Revised - 03/2015

Minimum Necessary – Johnny's Treatment Team

- Johnny is a 15 year old individual diagnosed with major depression and substance dependence. He was recently removed from his home and is now in a residential treatment program.

  Johnny has an appointment with Dr. Martins today at 4.

Revised - 03/2015

Minimum Necessary – Johnny's Mother's Treatment Team

-

  mother receiving mental health and financial assistance services from DHS.

  .

Revised - 03/2015

Minimum Necessary – EID Public Assistance – Johnny's Parents

-

mother and father are receiving (another service) and financial assistance services from DHS.

Revised - 03/2015

Challenges

Revised - 03/2015

Arlington County DHS HIPAA Compliance

The following procedural guidelines apply specifically to *all* Arlington County DHS employees, volunteers & students...

Revised - 03/2015

Authorizations – Release of Protected Health Information Form

- When to use the form
- Instructions on how to use the form
- Retention of the form

Revised - 03/2015

Vocal, Telephone & Voice Mail

- Do not discuss PHI in public areas within the workplace, such as elevators, reception areas, break rooms or outside the building
- Do not play back voice mail messages using speakerphone; any voice mail message may contain PHI which could be overheard by an unauthorized person
- Voice mail should be password protected. Do not share your voice mail password with anyone or post your password where it can be readily found, e.g. do not tape it to your desk, side of your computer, etc.

Revised - 03/2015

Work Area

- Do not leave papers that contain PHI lying around where unauthorized people can view them
- Paper documents that do not have to be retained must be shredded prior to disposal or placed in the locked shred bins
- At the end of the work day, secure all PHI within your desk and file cabinets – remember to **lock** all desk and file drawers. During non-working hours PHI should be reasonably secured from intentional or unintentional disclosure
- VDSS requires all visitors to be accompanied by DHS staff at all times
- Photographs have the same protection as other records

Revised - 03/2015

Personal Computer

- Files and documents containing PHI should be saved on a secure drive (U: or L:). Do not save PHI onto your hard drive (C:), a diskette or flash drive as PHI would no longer be password protected
- *All* computer, databases or networks containing PHI should be password protected
- Do not share your password with anyone; do not post or keep a copy of your password where it can be easily located
- Use a password protected screen saver when your computer is not in use. Activate the screensaver when leaving your work area or, at a minimum, set the screensaver for 15 minutes
- Position your computer screen so it does not face a hallway or visitors.
- Do not browse the DHS system for friends and neighbors
- Do not install software without DTS approval

Revised - 03/2015

Email/Outlook

- **Arlington County's email system is now encrypted!**
- ***How it works:***
  - In Outlook, mark the email sensitivity as confidential. This encrypts both the message content and any attachments
  - The subject line is not encrypted, so existing rules prohibiting protected information in the subject line remain in place
  - The recipient will receive a County formatted email indicating that they need to go to a Microsoft secure email portal to view the message.
  - Recipients will be able to reply, including with attachments, to the sender of the email. Note that the email thread must begin with a confidential email from our Outlook system.
  - Here is a guide: https://arlingtonva.sharepoint.com/tech/Shared%20Documents/Internal%20Email%20Encryption%20Training%20Manual.pdf
- Do not share your password with anyone or post your password where it can be readily found
- Do not put individual's names within your Outlook calendar

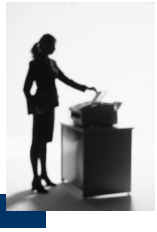
Revised - 03/2015

Social Networking

- Do not “friend” clients or parents
- Do not accept “friend requests” from clients or their family
- Do not discuss clients in public forums
- Do not post pictures of clients
- Be cautious on list serves, professional sites, etc.

Revised - 03/2015

FAX



- All PHI sent via facsimile should include a cover sheet containing a statement of confidentiality. Contact the recipient immediately before and after sending the fax to ensure that it is expected and picked up promptly
- All PHI received via fax should be promptly picked up and secured by staff
- Fax machines should be located in an area where an accountable person can ensure that faxes are kept confidential and PHI is distributed to the proper recipients
- PHI received via fax should not be posted or pinned to bulletin boards in common areas awaiting distribution
- Misdirected Faxes require an Incident Report

Revised - 03/2015

Mail

- Make sure that opened mail which contains PHI is not left sitting in a public area or in an unsecured mailbox
- Incoming mail should be delivered directly to the recipient or picked up from the mailroom by an accountable person in each work unit and kept secure, until it can be distributed to the recipient
- Use a sealed envelope to send all outgoing mail that contains PHI

Revised - 03/2015

Off-Site

- PHI that is used off-site should be secured when not in use, i.e. locked bag
- Reasonably safeguard PHI from intentional or unintentional disclosure from unauthorized people (This includes family members and guests)
- Car, elevator, home, bathrooms

Revised - 03/2015

Remote Access

- Work space meets Arlington County guidelines on AC Source
- Secure all PHI when not supervising or using your PC
- Paper documents containing PHI should not be brought home
- Secure AC log-on password
- Use only the One Drive or the telework portal; do not save PHI to your own PC
- Be mindful of protecting PHI while working in public places, e.g. Starbucks, Panera, etc.

Revised - 03/2015

Integrated Services

- **HIPAA Does Not Prevent Us from Providing Integrated Services**
- "A covered entity that is a government agency administering a government program providing public benefits may disclose protected health information relating to the program to another covered entity that is a government agency administering a government program providing public benefits if the programs serve the same or similar populations and the disclosure of protected health information is necessary to coordinate the covered functions of such programs or to improve administration and management relating to the covered functions of such programs." 45 CFR 164:512(k)(6)(ii)
- **HOWEVER HIPAA does require that we:**
- **Limit information to the minimum necessary to achieve the goal**
- **Share information with only those employees who have a need to know the information**
- **Notify the client of our practices and give them the option to object**

Revised - 03/2015

If you have questions….

Please contact your divisional representative

• Longman, Jan	DO/Compliance/Privacy Officer	x1613
• Thomas, Marianne	DO/Compliance	x1693
• Smith, Nicole	DO/Compliance	x1605
• Terrell, Dwaine	Records/Archives	x1672
• Compliance Hotline	DO/Compliance	x2667 (703-228-COMP)

iLink

For Training Materials, Records Management Policy(s), Instructions for Completion of Authorization for Release of PHI and other related information

AC Commons

Administrative Regulations – Health Insurance Portability and Accountability Act of 1996

Revised - 03/2015