HIPAA
Basic Training 2015

Susan Barker Andrews, J.D. CHPC
Kahlea Porter, J.D.

KDADS Staff HIPAA/Security Training

Purpose of Training:

To ensure the privacy and protection of health information belonging to individual's served by KDADS and to comply with Federal law and regulations!

Goal of Training:

To provide all staff with updated HIPAA/Security training and provide a better understanding of how to safeguard KDADS' consumer's protected health information.

Consequences of failure

KDADS is currently updating the employee handbook. HR policies are posted on the intranet as they are updated. Under the Secretary's Directive former KDOA policies remain in effect until replaced.

Bottom Line: ***"Your employment may be terminated if you improperly use or disclose PHI in a manner that is not authorized by KDADS."***

See KDADS Employee Handbook: Section 4.1.C (HIPAA) and Section 16 (Information Security).

What is HIPAA?

- HIPAA stands for: **Health Insurance Portability and Accountability Act**
- HIPAA is a large act that made several changes to health and insurance law
- Title II of the Act
  - Administrative Simplification standards and requirements *(Sections 261 through 264)*
  - Created new rules for the protection of individual health information

Health Insurance Portability and Accountability Act of 1996, Public law 104-191

Administrative Simplification

- Created to improve efficiency and effectiveness of healthcare systems by standardizing the electronic exchange of clinical and administrative data.
- Attempts to improve security of individual health information.
- Attempts to safeguard the confidentiality of protected health information and protect the integrity of health data while ensuring the availability of care

Who does it apply to?

- HIPAA standards only apply to what are called **Covered Entities** within HIPAA.
- Covered Entities include, but are not limited to:
  - **Health Care Providers**
    - Doctors, hospitals, etc.
  - **Health Plans**
    - Kansas Medicaid
    - Medicare
    - State Employee Health Plan
  - **Health Care Clearinghouses**
    - Entities that transfer data on behalf of providers or plans
  - **Hybrid Entities**
    - A single legal entity where only some of the divisions or programs meet the definition of a Covered Entity.
      - KDHE and KDADS are examples of Hybrid Entities

See 45 CFR 164.103

PRIVACY RULE

45 CFR Parts 160 and 164 (the "HIPAA Security and Privacy Rule") Protected Health Information (PHI)

PHI is health information collected from an individual, created or received by a covered entity and:

- Relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and
- That identifies the individual;
- There is a reasonable basis to believe the information can be used to identify the individual.

Privacy Rule
What PHI is protected?

The Privacy Rule protects all PHI held or transmitted by a covered entity or its business associate in any form or media, whether electronic, paper or oral.

Privacy Rule

- Provides a standard level of privacy protections of Protected Health Information (PHI).
- State laws that are contrary are preempted by the Federal law. *(45 C.F.R. §160.203)*
  - Permits more stringent state laws to remain in effect. A number of states have more stringent privacy laws. *(Examples include MN, NY)*
- Limits how PHI may be **used or disclosed**.

Privacy Rule – Use and Disclose

- **Use**: Means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information. *(45 C.F.R. §164.502(a))*

- **Disclose**: Means the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information. *(45 C.F.R. §164.502(a)(2))*

- A Covered Entity may not **use or disclose** PHI, except as permitted or required by the Privacy Rule.

Privacy Rule – Use and Disclose

- Covered Entities are **required** to disclose PHI to:
  - The individual who owns the PHI when requested by the individual.
    - KDADS employees are required to verify that they are speaking to the individual who owns the PHI before releasing the information.
  - The Secretary of the U.S. Department of Health and Human Services (HHS) for HIPAA investigations and compliance with the Privacy Rule.

See 45 CFR 164.502

See KDADS Employee Handbook: 4.1.C (HIPAA policy)

Privacy Rule – Use and Disclose

- Covered Entities are **permitted** to use or disclose PHI with a valid authorization from the individual.

- Unless an exception is met, in order to use and/or disclose PHI, an authorization must be in writing. To have a valid authorization the following must be including in the written document:
  - Description of the PHI to be used or disclosed that identifies the PHI in a specific manner
  - Specific description of who can use the PHI
  - Specific description on who the covered entity can provide the PHI to
  - Specific description of each purpose of the request

Privacy Rule – Use and Disclose

- Written Authorization requirements (continued)
  - Expiration date for request
  - Signature of the individual or personal representative
  - The following statements must be included in an authorization:
    - Inform the individual they have the right to revoke the authorization at any time
    - Whether participation is condition on signing authorization
    - Potential for information to be re-disclosed by a person or entity receiving the PHI

Privacy Rule – Use and Disclose

- Authorization (continued)
  - A copy of the authorization must be provided to the individual
  - Your division/commission should have a standard authorization form to use
  - If you have a question regarding authorization forms you should contact the KDADS' Legal Division

Privacy Rule – Use and Disclose

- Covered Entities are permitted to use and disclose PHI without authorization for essential health care functions:
  - Treatment
  - Payment
  - Operations

See 45 CFR 164.506

Privacy Rule – Use and Disclose

- **Treatment**: Means the provision, coordination, or management of health care usually by health care providers
  - A typical example is when a health care provider discusses a patient's care with another provider within the same office

Privacy Rule – Use and Disclose

- **Payment**: Means activities of covered entities to obtain payment, premiums, fulfill coverage responsibilities or provide reimbursement for the provision of health care
  - Example: A health plan can provide PHI information to a hospital in order to coordinate payment of a claim

Privacy Rule – Use and Disclose

- **Operations**: Means administrative, financial, legal and quality improvement activities of a covered entity
  - Necessary to run the business of the covered entity
  - Includes:
    - Quality assessment, training, accreditation, certification, licensing, evaluating performance, fraud and abuse detection; and
    - Underwriting, rating, coordination of benefits, legal services, business management

Privacy Rule
Permissible Uses or Disclosures

- Covered Entities are permitted to use or disclose PHI for reasons including, but not limited to:
  - Public Health Activities (ex. Vital statistics, FDA reporting)
  - Health Oversight (ex. Entities authorized to oversee a healthcare system)
  - Law Enforcement (ex. For victims of a crime)
  - Workers' Compensation
  - Report Abuse and Neglect
  - Legal Proceedings (ex. Court Order, Discovery Request, Subpoenas)
  - Special Government Functions (ex. Military programs, national security)

- **Before you use or disclose PHI for one of these reasons, you must contact the Legal Division immediately!**

Privacy Rule

- Accounting of disclosures
  - Covered Entities must maintain an accounting of most disclosures of PHI
  - This does not have to include disclosures made for treatment, payment, operations, a limited data set, or with an authorization
  - Please see the KDADS Employee Handbook 4.1.C (HIPAA policy) for how to document disclosures

Privacy Rule – Use and Disclose

- Covered Entities may use PHI to create information that is not PHI by **de-identifying** the information by removing certain data elements.

- The HIPAA regulations list the specific data elements that must be removed before the PHI is to no longer be considered PHI. These include, but are not limited to:
  - Names, dates, geographic subdivisions smaller than a state, telephone numbers, email addresses, medical record numbers, health plan identification numbers, account numbers, social security numbers, etc.

See 45 CFR 164.514

Privacy Rule – Use and Disclose

- Covered Entities are permitted to use or disclose a **limited data set** if the Covered Entity enters into a data use agreement by removing certain data identifiers listed in HIPAA regulations.

See 45 CFR 164.514(e)

Privacy Rule – Minimum Necessary

- When Covered Entities do use or disclose PHI, they are required to make reasonable efforts to only use or disclose PHI in a **minimum necessary** amount to accomplish the intended purpose
  - Good rule of thumb: Less is best. Whatever the least amount of PHI required to accomplish legitimate purpose should be used!
  - *See* 45 CFR 164.502

Privacy Rule – Breach

Privacy Rule – Breach

- Don't panic! You do not have to make the call as to whether a breach has occurred.
  - Immediately contact your supervisor **and** KDADS Legal Department so that we can analyze whether a breach has occurred.
- If there is a breach of PHI, Covered Entities are required to notify certain people and there is a limited amount of time in which to do so; therefore time is of the essence!

Privacy Rule – Breach

- What is a breach of PHI?
  - A breach is any unauthorized acquisition, access, use or disclosure of unsecured PHI which compromises the privacy or security of PHI
    - Examples: Theft or lost laptop that contained PHI; theft or lost paper files that contained PHI; employee disclosing member PHI to spouse about ex-spouse; etc.
  - Unsecured PHI means PHI that is not secured through technology or a method required by HIPAA
    - Examples: Emailing PHI in an unsecure manner/unencrypted to someone outside the Covered Entity; Not storing data behind a firewall; Storing PHI unprotected on a laptop

See generally 45 CFR 164.402

Privacy Rule – Breach

- Breach Notification
  - If it is determined there was in fact a breach the Covered Entity must notify the individual or personal representative without reasonable delay and no later than 60 days
  - **Individual employees are not to start the process of notification without specific instructions from the KDADS Legal division or the HIPAA Compliance Officer**.

Privacy Rule – Breach

- If the breach puts the individual in imminent danger the Covered Entity must notify by phone
- If breach involves the use or disclose of more than 500 people the Covered Entity must also notify prominent media in the area as well as the Secretary of HHS
- **Individual KDADS employees may not speak to the media without permission from the Communications Division and the Legal Division.**

Privacy Rule – Administrative Requirements

- The Privacy Rule does require Covered Entities to establish and provide the following:
  - Designate a Privacy Official
  - Train all members of the work force who have the ability or means to view/access/create PHI
  - Safeguard PHI physically and technologically
    - Use shredding services, keep PHI under lock and key, keep a visitor log of non-employee visitors, etc
  - Develop policies and procedures for the Covered Entity to protect PHI
  - Create a method for individuals to be able to report potential privacy violations
  - Develop sanctions and consequences for violations of privacy policies and procedures by staff

WHAT SHOULD A KDADS STAFF MEMBER DO IF THEY SUSPECT A *POTENTIAL* BREACH?

ANSWER: **REPORT IT** TO SUPERVISOR AND TO THE PRIVACY OFFICERS IN THE KDADS LEGAL DIVISION

- susan.andrews@kdads.ks.gov and
- kahlea.porter@kdads.ks.gov and
- karla.werth@kdads.ks.gov

Security Rule

Security Rule

- Security Rule defines how to protect PHI in electronic form
- The Security Rule only applies to PHI maintained or transmitted in electronic form, or ePHI
  - In contrast, the Privacy Rule regulates all forms of PHI whether in electronic, written or oral form

Security Rule

- The Security Rule requires Covered Entities to have **Administrative, Physical and Technical Safeguards** in place
  - These must be contained within the Covered Entities policies and procedures
  - HIPAA does not require specific things or actions a Covered Entity must do
  - The Security Rule is intended to be technologically neutral by only outlining principles and not requiring single solutions

Security Rule

- Administrative, Physical and Technological (continued)
  - Therefore, Covered Entities are left to follow best practices when attempting to comply with the Security Rule
  - Examples include:
    - Password protection for computers
    - Encrypt email
    - Storing PHI behind electronically locked doors
    - Requiring employees to wear ID badges at all times
    - Using badge ID doors

Security Rule

- It is your responsibility to help ensure that only individuals with valid authorization enter KDADS secure areas.
  - Your key card/fob only grants **you** access to the KDADS secure areas, not those who may attempt to piggyback or tailgate in behind you.
  - **DO NOT** make yourself responsible for allowing others access into secure areas.

Security Rule

- Administrative, Physical and Technological safe guards (continued)
  - Track the use of all laptops that may contain PHI
  - Encrypt and password protect all laptops that may contain PHI
  - Conduct security awareness training of all workforce members (including management)
  - Monitor log-in attempts and report discrepancies

Electronic Device Security

All KDADS computers and tablets are password protected. The passwords change every sixty (60) calendar days.

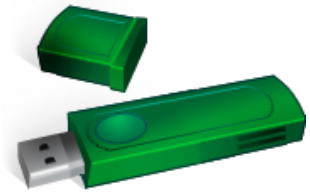
- The passwords must be 8 characters long, and include at least one numeric digit, one lower case letter, and one upper case letter.
- When you leave your workstation lock your computer by pressing the Window key and the “L” key at the same time. To unlock the screen press “Ctrl”, “Alt”, and “Delete” at the same time.

Data Security

- All PHI must be secured within the network drives designated for your Commission. Saving your files to the appropriate network will ensure that the data can only be accessed by person with the same security access.

- DO NOT save PHI on your desktop.

Thumb/Flash Drives



KDADS has taken appropriate steps to password and encrypt thumb/flash drives.

KDADS staff members who have a thumb/flash drive, or seek to check out a KDADS thumb/flash drive, will be given a copy of the encryption directions and asked to review them.

KDADS IT support and technical assistance will be available if required.

Paper Files

KDADS is steadily becoming a “paperless” entity, the use and transport of paper files should be minimal.

During 2013 KDADS contracts and background checks were converted to near paperless web based applications.

Staff still using paper files are required to keep them locked up when not under immediate control. This includes PHI that is physically moved from one location to another.

Security Rule

- Security Incident
  - Covered Entities are required to identify and respond to all Security Incidents
    - A Security Incident is any attempted or successful unauthorized access, use, disclosure, modification or destruction of ePHI
    - **Contact your supervisor and the Legal Division immediately!**

HITECH

The American Recovery and Reinvestment Act of 2009 (Public Law 111-5) Title XIII of Division A and Title IV of Division B, called the "Health Information Technology for Economic and Clinical Health" (the "HITECH ACT") provided modifications to the HIPAA Security and Privacy Rule.

Overview of the Omnibus Final Rule

- Modified HIPAA to implement the statutory amendments of the Health Information Technology for Economic and Clinical Health Act (**HITECH Act** *or just* **HITECH)**
- HITECH brought Business Associates under the requirements of the Privacy and Security Rules
- Imposes data breach notification requirements for unauthorized use or disclosure of unsecured PHI
- Increased the penalties for violations and breaches of the Privacy and Security Rules
- Some other modifications to the HIPAA Rules were included to improve their workability and effectiveness.
- Implemented modifications required by the Genetic Information Nondiscrimination Act of 2008 (**GINA).**

Refresher/Update on BAs

Business Associate (BA): The HIPAA Rules generally define a BA as a person who performs functions or activities on behalf of, or certain services for, a CE that involve the use or disclosure of PHI.

The Omnibus Final Rule expressly added:

(1) Health Information Exchange Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to PHI to a CE and that requires routine access to such PHI and

(2) (2) A person who offers a personal health record to one or more individuals on behalf of a CE.

See 45 CFR 160.103
(Note BAs can be covered entities under 45 CFR 160.103(2))

For an example of two business associate agreements posted to the KDADS website go to: http://www.aging.ks.gov/Forms/Forms_index.html

Enforcement Of HIPAA

HIPAA Enforcement

- The Office of Civil Rights (OCR) has the authority to investigate and enforce the Privacy and Security Rules of HIPAA
- CMS – Investigates and enforces transactions and code set violations
- DOJ – Investigates Privacy Criminal complaints
- State Attorney Generals have authority to bring claims under HIPAA
  - Kansas Attorney General Office has chosen to not participate

HIPAA Enforcement–4 Penalty Tiers

Violation category	Each violation	All identical in a calendar year
Did Not Know	$100–$50,000	$1,500,000
Reasonable Cause	$1,000–50,000	$1,500,000
Willful Neglect–Corrected*	$10,000–50,000	$1,500,000
Willful Neglect–Not Corrected	$50,000	$1,500,000

*An affirmative defense applies under 45 C.F.R. 160.410 when an entity corrects the violation within 30 days from the date the entity had knowledge or would have had knowledge with the exercise of reasonable diligence.

30 -day cure period

The 30-day cure period begins on the date that an entity first acquires actual or constructive knowledge of the violation and will be determined based on evidence gathered by HHS OCR during its investigation, on a case-by-case basis.

More Information

http://www.hhs.gov/ocr/privacy/index.html
The Office for Civil Rights enforces

- The HIPAA Privacy Rule: which protects the privacy of individually identifiable health information;
- The HIPAA Security Rule: which sets national standards for the security of electronic protected health information; and
- The confidentiality provisions of the Patient Safety Rule: which protect identifiable information being used to analyze patient safety events and improve patient safety.

Definition of Workforce

"Workforce" as defined at 45 CFR 160.103, means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate.

Who is responsible and What can YOU do????

1. Who is responsible for KDADS HIPAA Compliance?
   - The entire workforce.

2. What can YOU do?
   - Ask questions
   - **Double check** every fax and email to verify, the correct number, address and whether the PHI is limited to the minimum necessary for the KDADS business purpose.

3. Educate yourself.
   - Take a look at the HHS OCR website to gain a basic understanding. Yes, they have FAQs.

4. **Ask yourself** if you would treat your own or your parent's PHI that way.

What YOU can do continued

- Always **encrypt** when emailing PHI outside KDADS including communications to KDADS BAs.
- **Think** about where you leave information. Don't leave PHI laying around near fax machines, copiers, on conference tables or wherever your eyes are not on it and it is not secure/locked up.
- **Report** concerns and suggestions to your supervisor and to the KDADS Legal Division, Attention: Privacy Officer. Don't stop there. Follow up to find out if the concerns and suggestions were addressed or acted upon.

What YOU can do continued

- **Don't hesitate** to go up the chain of command in reporting potential HIPAA concerns. Follow up on your report with your supervisor and the KDADS Legal Division.

Contact info:
susan.andrews@kdads.ks.gov
kahlea.porter@kdads.ks.gov

Please Copy Legal Assistant karla.werth@kdads.ks.gov

If Susan Andrews or Kahlea Porter are not available contact any other KDADS counsel. If you have the wrong person they will direct you elsewhere.

- **Don't wait**. The stakes are **too high** and **HIPAA can't wait.**

The end…

- Until Next Review