HIPAA Demystified: A Simple Approach to Building a HIPAA Compliance Program Including HITECH and TMPA.

EPCC Health Career and Technical Education

November 1, 2012

What is HIPAA & why should I care?

- HIPAA, aka the Health Insurance Portability and Accountability Act, was first enacted in 2003. It was followed by Security and Privacy Rules in 2004.

- The HITECH Act, enacted in 2009, requires any entity that handles protected health information (PHI) to report breaches, whether in paper or electronic form. For colleges and universities with employee health plans or student health centers, this means complying with various aspects of the HIPAA privacy, security, and HITECH rules.

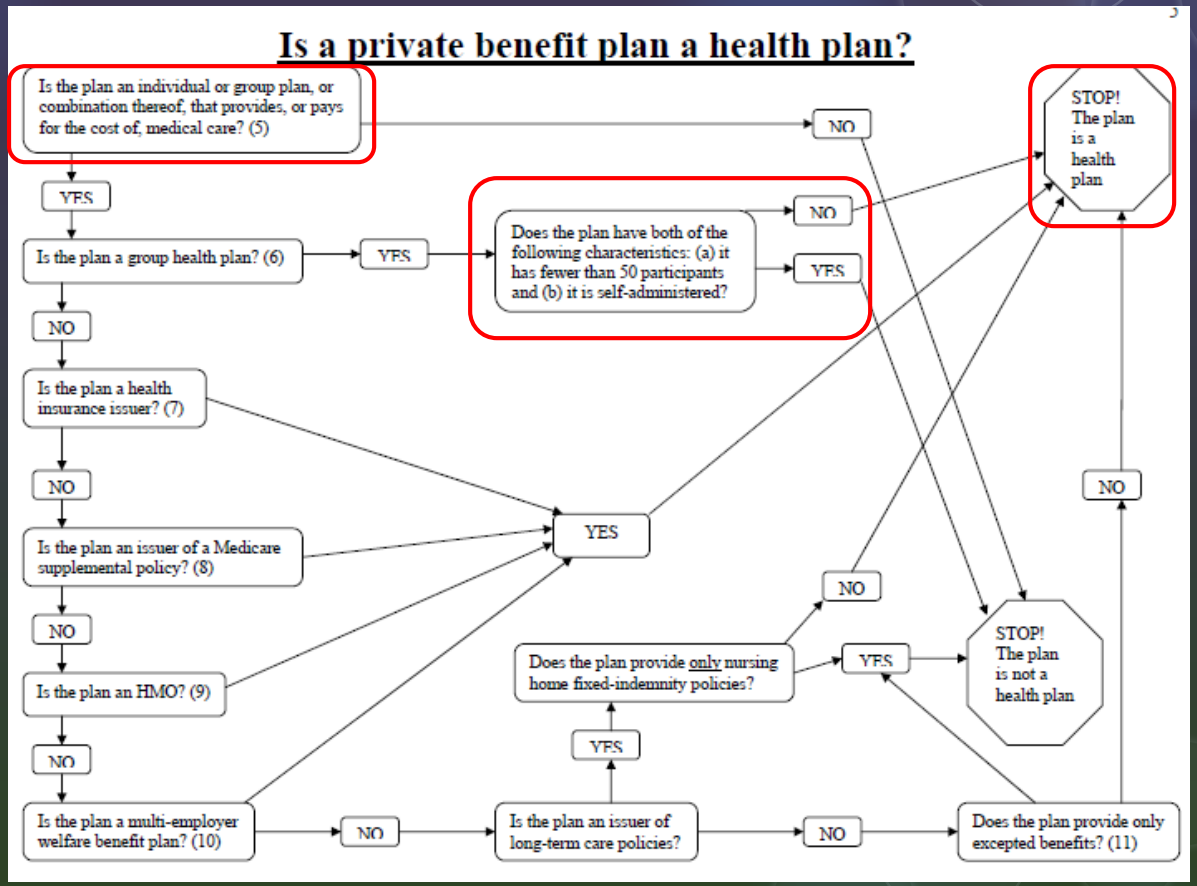
What is HIPAA & why should I care?

- It is very important to make a good faith effort to protect PHI. Civil penalties can be up to $100 for each offense (with a cap of $25,000 per year for multiple offenses), and criminal penalties can be up to $250,000 and/or 10 years in prison for deliberate, wrongful misuse of personal health information

What does that mean for me?

- If you have an:
  - Employee Sponsored Health plan and more than 50 employees; or
  - Section 125 Plan and more than 50 employees (even if fulfilled through a vendor)
  - A Hybrid entity(Clinic and school)

HIPAA applies to you!



Source: https://www.cms.gov/HIPAAGenInfo/Downloads/CoveredEntitycharts.pdf

How did HITECH change the game?

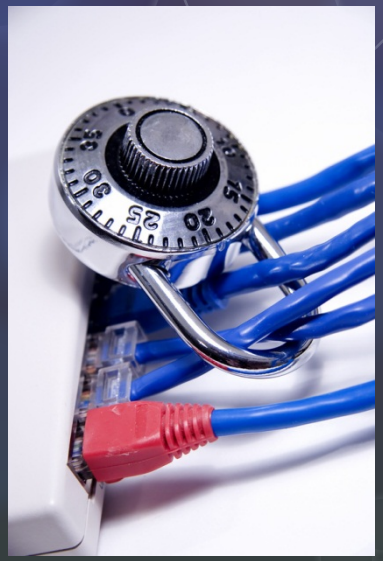
- As part of the American Recovery and Reinvestment Act of 2009, legislation called the Health Information Technology for Economic and Clinical Health Care Act (HITECH Act) and was also passed then.
- You are now required to report a breach of PHI if it occurs.

How did HITECH change the game?

- There are additional privacy and security requirements.
- Business Associates (anyone external vendors that handle PHI) are also bound by the HIPAA Security and Privacy rules.
- For medical institutions, it establishes a timeframe for the use of electronic health records by 2014

What is a breach?

- "Breach" means unauthorized access, acquisition, use or disclosure of protected health information which compromises the security or privacy of that information.
  - If an employee opens mail with PHI, but that employee is not on the designate access list for PHI, is this a breach?
  - If a laptop with PHI is lost, but not encrypted, is that a breach? Is it a breach if the laptop is encrypted?



Source: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html

What is unsecured PHI?

- "Unsecured PHI" means PHI that is not secured through use of a technology or methodology identified by the U.S. Department of Health and Human Services (HHS) as rending the informant unusable, unreadable, or indecipherable to unauthorized persons.
- Encryption of data at rest and in transit.
- Scrubbing that uses DOD standards for electronic data when reused, sold or destroyed.

- Source: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html

What are the breach notification requirements?

- Notification is required to the affected individuals, the government and in some cases, the media in the event of a breach of "Unsecured Protected Health Information."
- Breach requirements are applicable to both "covered entities" and their "business associates."
- If your BA(Business Associate) has a breach, you need to report it.

Breaches Affecting 500 or More Individuals

As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals. These breaches are now posted in a new, more accessible format that allows users to search and sort the posted breaches. Additionally, this new format includes brief summaries of the breach cases that OCR has investigated and closed, as well as the names of private practice providers who have reported breaches of unsecured protected health information to the Secretary. The following breaches have been reported to the Secretary:

Full DataSet CSV format (18 KB) XML format (57 KB)

Select a column head to sort by that column. Select again to reverse the sort order. Select an individual record to display it in full below the table.

Filter: university 24 records showing

Name of Covered Entity	State	Individuals Affected	Date of Breach	Type of Breach	Location of Breached
Brown University	RI	528	2009-12-11	Unauthorized Access/Disclosure	Paper Records
Georgetown University Hospital	DC	2,416	2010-03-26	Theft	E-mail, Portable Electronic Device
Johns Hopkins University Applied Physics Laboratory Medical and Dental Insurance Plan	MD	692	2010-06-15	Unauthorized Access/Disclosure	E-mail
Loma Linda University Health Care	CA	584	2010-04-04	Theft	Desktop Computer
Loma Linda University School of Dentistry	CA	10,100	2010-06-13	Theft	Desktop Computer
New York Presbyterian Hospital and Columbia University Medical Center	NY	6,800	2010-07-01	Hacking/IT Incident	Network Server
The University of Texas at Arlington	TX	27,000	2010-02-19	Hacking/IT Incident	Network Server
Thomas Jefferson University	PA	21,000	2010-06-14	Theft	Laptop

Breach notification is required within 60 days of finding that a breach occurred.

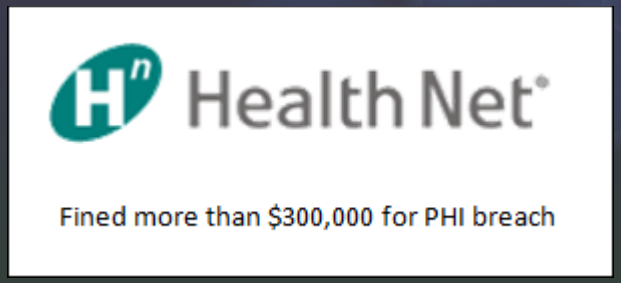
Source:
http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html

What happens if my BA(Business Associate) has a breach:

- Business Associates must notify their covered entity in the event of a breach.
- The timing is still only 60 days to report the breach, so make sure your BA notifies you in a timely manner.
- Work with your BA to assess what happened, how it happened, who is affected and how to correct it for the future.
- You must send the letter to affected parties.
- You will be listed on the HHS site if more than 500 individuals (not the BA).

What happens if I don't comply?

- There are stiff penalties for non-compliance, ranging from fines of $100 to $50,000 per violation, capped at $25,000 to $1.5 million per violation of the same standard.
- Criminal penalties of 1 to 10 years in jail for gross negligence.
- HITECH created new avenues for enforcement, allowing state attorney generals to enforce HIPAA regulations.
- CT attorney general brought a suit against Health Net for a breach of data on 1.5 million customers and won the suit.
- VT Attorney announced he also settled a lawsuit against Health Net for $55,000.



So, what is PHI?

- Names;
- All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code
- All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; Telephone numbers;
- Fax numbers;
- Electronic mail addresses;
- Social security numbers;
- Medical record numbers;
- Health plan beneficiary numbers;

Source: http://www.hipaa.com/2009/09/hipaa-protected-health-information-what-does-phi-include/

What is PHI?

- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints;
- Full face photographic images and any comparable images; and
- Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section;

- Source: http://www.hipaa.com/2009/09/hipaa-protected-health-information-what-does-phi-include

What is a covered transaction?

45 C.F.R.162.1101: Health care claims or equivalent encounter information transaction is either of the following:

(a) A request to obtain payment, and necessary accompanying information, from a health care provider to a health plan, for health care.

(b) If there is no direct claim, because the reimbursement contract is based on a mechanism other than charges or reimbursement rates for specific services, the transaction is the transmission of encounter information for the purpose of reporting health care.

Source: https://www.cms.gov/HIPAAGenInfo/Downloads/CoveredEntitycharts.pdf

What is a Covered Transaction?

- 45 C.F.R.162.1401: A health care claim status transaction is the transmission of either of the following:
- (a) An inquiry to determine the status of a health care claim.
- (b) A response about the status of a health care claim.

- 45 C.F.R.162.1501: The enrollment and disenrollment in a health plan transaction is the transmission of subscriber enrollment information to a health plan to establish or terminate insurance coverage.
- Source: https://www.cms.gov/HIPAAGenInfo/Downloads/CoveredEntitycharts.pdf

What is a Covered Entity?

- 45 C.F.R.162.1301: The referral certification and authorization transaction is any of the following transmissions:
- (a) A request for the review of health care to obtain an authorization for the health care.
- (b) A request to obtain authorization for referring an individual to another health care provider.
- (c) A response to a request described in paragraph (a) or paragraph (b) of this section.
- Source: https://www.cms.gov/HIPAAGenInfo/Downloads/CoveredEntitycharts.pdf

What is a Covered Transaction?

- 45 C.F.R.162.1201: The eligibility for a health plan transaction is the transmission of either of the following:
- (a) An inquiry from a health care provider to a health plan or from one health plan to another health plan, to obtain any of the following information about a benefit plan for an enrollee:
- (1) Eligibility to receive health care under the health plan.
- (2) Coverage of health care under the health plan.
- (3) Benefits associated with the benefit plan. (b) A response from a health plan to a health care provider's (or another health plan's) inquiry described in paragraph (a) of this section.
- Source: https://www.cms.gov/HIPAAGenInfo/Downloads/CoveredEntitycharts.pdf

What is a covered transaction?

45 C.F.R.162.1601: The health care payment and remittance advice transaction is the transmission of either of the following for health care:

(a) The transmission of any of the following from a health plan to a health care provider's financial institution:

(1) Payment.

(2) Information about the transfer of funds.

(3) Payment processing information.

(b) The transmission of either of the following from a health plan to a health care provider:

(1) Explanation of benefits.

(2) Remittance advice.

45 C.F.R.162.1701: The health plan premium payment transaction is the transmission of any of the following from the entity that is arranging for the provision of health care or is providing health care coverage payments for an individual to a health plan:

(a) Payment.

(b) Information about the transfer of funds.

(c) Detailed remittance information about individuals for whom premiums are being paid.

(d) Payment processing information to transmit health care premium payments including any of the following:

(1) Payroll deductions.

(2) Other group premium payments.

(3) Associated group premium payment information.

45 C.F.R.162.1801: The coordination of benefits transaction is the transmission from any entity to a health plan for the purpose of determining the relative payment responsibilities of the health plan, of either of the following for health care:

(a) Claims.

(b) Payment information.

Source: https://www.cms.gov/HIPAAGenInfo/Downloads/CoveredEntitycharts.pdf

Where do I start?

- Find out what PHI you process, where it comes from, where it goes and how you store it. Start with HR and your health center/medical facilities.
- Build a flow to help others understand where that information resides and have internal or external counsel confirm if your assumptions are correct.

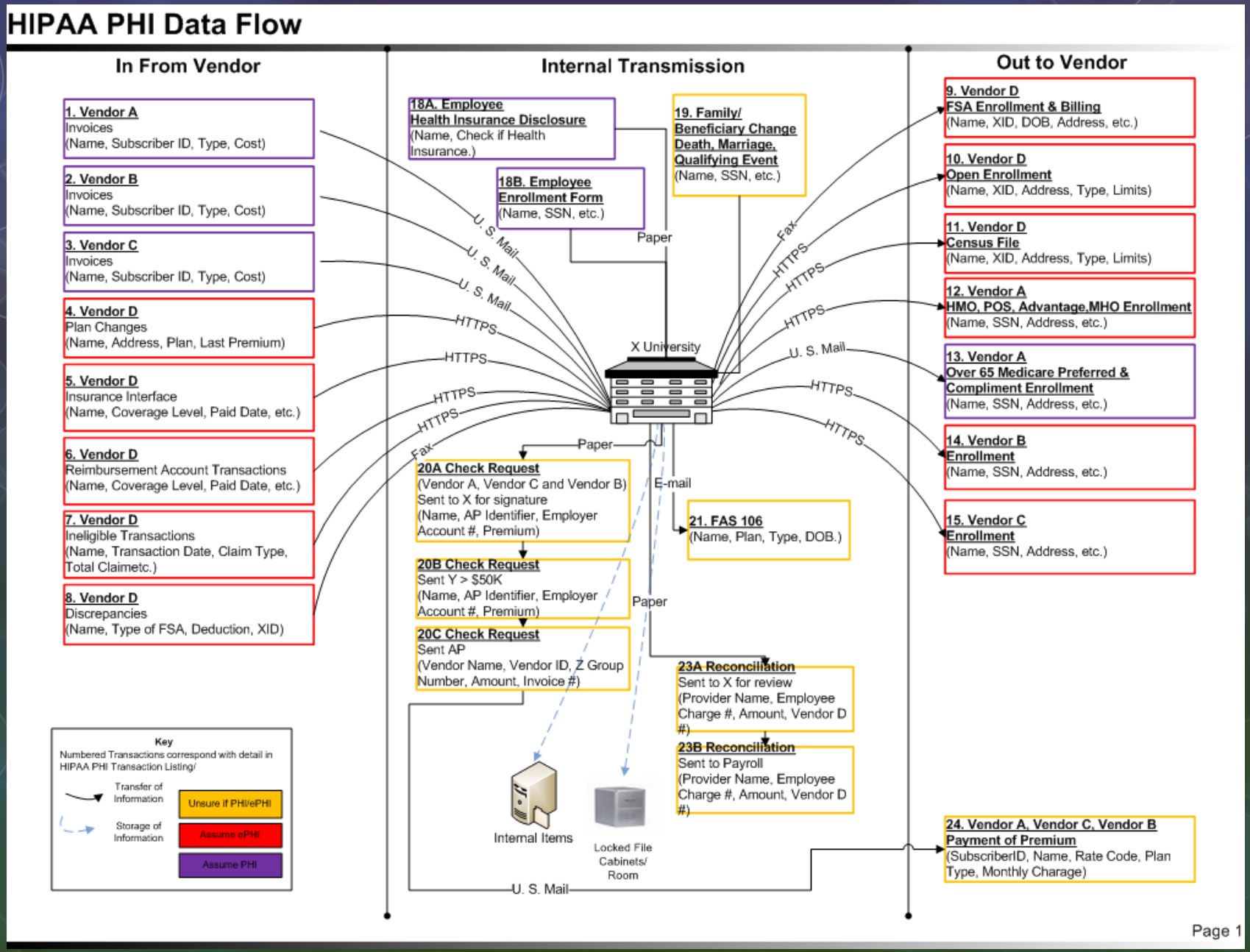
Ask the following questions:

- What information do we exchange with our health and dental plans in paper form? Where do we store this information? Is it separate from other employee information?
- What information do we exchange with our health and dental plans in electronic form? Where do we store this information?
- Who are our Business Associates? Do we have BA agreements on file for each one?
- What information do we exchange with our BA's in paper form? Where do we store this information?
- What information do we exchange with our BA's in electronic form? Where do we store this information?
- Do we disclose PHI about individuals? If so, how is it used (other than criminal activity or legal obligation)? Who tracks disclosures and how?

Ask the Following Questions: (2)

- Do we disclose PHI in situations that might require authorization? If so, do we:
- Do we track disclosures of ePHI now (defined as disclosures to third parties for treatment, payment and healthcare operations)? Or do we not disclose information on any of these items? Disclosure could be for law enforcement, judicial, coroner, etc.
- Do we require employees to sign an authorization form to disclose PHI? If so, were do we keep these and then what types of information do we disclose? Do we have a special authorization form for this purpose?
- Who has access to the PHI we store in paper form?
- Who has access to the PHI we store in electronic form?
- Do we share PHI or EPHI with staff outside of HR?
- Do we have HIPAA training in place? Who is required to take it?
- Do we have Information Security training in place? Who is required to take it?

Build a Data Flow



Assessment Results

- Create a matrix that corresponds to your diagram. List all data elements collected to see if you can determine if the information is PHI.
- Use this this grid and the diagram to review with internal stakeholders and appropriate HIPAA experts.

HIPAA PHI Transactions

The below transactions correspond with the numbered items on the HIPAA PHI Data Flow for X University diagram. In the column labeled "Is PHI", we have entered a "Y" in areas that we are believe are PHI and a "?" in areas that we are unsure of.

#	Event Name	Received From/Sent To	Data Elements	Is PHI?
1	Vendor A Invoices	Vendor A	Name, Subscriber ID, Type, Cost	Y
2	Vendor B Invoices	Vendor B	Name, Subscriber ID, Type, Cost	Y
3	Vendor C Invoices	Vendor C	Name, Subscriber ID, Type, Cost	Y
4	Vendor A Plan Changes	Vendor A	Name, Dependents, Gender, DOB, Coverage Effective Date, Address	Y
5	Vendor A Interface	Vendor A	Name, Coverage Level, Paid Through Date, Monthly Premium, Category (Retiree, Cobra)	Y
6	Vendor A Transaction Summary	Vendor A	XID, Name, Plan Type, Deposits, Claims, Payments and Balance	Y
7	Vendor A Ineligible Transactions	Vendor A	Name, Transaction Date, Claim Type, Total Claim amount, eligible Amount, amount approved, ineligible amount, denied amount,	Y
8	Vendor A Discrepancy Report	Vendor A	Name, XID, Pay Cycle (M, B), Date, Ded. Code (Medical or Dependent Care), Expected amount, Actual Amount, Difference, Reason for Discrepancy	Y
9	Vendor A Enrollment & Billing	Vendor A	Name, Gender, DOB, Home Address, Qualifying Event, Loss of Coverage Date, Termination Type, HIPAA Date, Coverage (Medical/Dental), Dependant Name, Dependant, DOB, Dependent Gender, Dependent Original Coverage Date, Dependent Address (sent via fax)	Y

Sample Breach Point Analysis

- Use the items from the risk assessment to determine where a breach could occur
- Discuss potential breach scenarios and ways to mitigate breach
- Understand that it is not possible to mitigate all breaches (i.e. paper lost in the mail).

Potential Breach Point	Potential Scenario	Comments
PHI stored in X	Lost key or potentially left unlocked.	Low risk. File is in internal .... Check cabinet at end of day. Have cabinet rekeyed if keys are lost.
EPHI stored on Servers	Information is hacked (by employee or outside source)	Encrypt data with X tool. Encryption will provide safe harbor.
PHI sent via U.S. Mail	Item is lost in the mail	Minimal impact if only 1 item sent at a time, but still needs to be reported as a breach. If more than 25 items, use Fed Ex direct signature service.
PHI sent via Fax	Item sent to wrong fax number	Minimal impact if only 1 item sent at a time, but still needs to be reported as a breach.
Items sent via HTTPS using vendor web site	Vendor site is hacked or experiences problems	Out of our control; must work with vendors to address
PHI received from employees	Employee sends via interoffice mail instead of hand deliver	All employees sign confidentiality agreements; should not be considered as breach.

Additional Items for Consideration:

- HIPAA regulations are very complex; someone other than you should review and ensure information is accurate.
- Review National Institute of Standards and Technology (NSIT) "An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule" document for additional details.

After you find your PHI, create policies & procedures:

- For the Privacy Rule, update your HIPAA Privacy Policy and post it to the web. Notification is required to appropriate parties every 2 years. Assign a security official who is responsible for development of policies and procedures.
- For the Security Rule,
  - Update or create HIPAA Procedure documents for anyone handling PHI.
  - Ensure that all employees that handle PHI participate in HIPAA training on a yearly basis.
  - Create or update your breach response plan.

The Security Rule: Required vs. Addressable

- A "required" implementation specification is similar to a standard. A covered entity (you) must comply with it.
- For "addressable" items, you must perform an assessment to determine if it is a reasonable and appropriate safeguard.
- For addressable items, you must document the assessments and all decisions.
- All EPHI created, received, maintained or transmitted by a covered entity is subject to the Security Rule.

Source: http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf

Procedures: Address the Administrative for ePHI:

- Risk Analysis
- Risk Management
  - PHI in paper form must be stored in a separate, locked area. The information can not be intermingled with employee files.
- Sanction Policy
- Information System Activity Review
- Assign Security Responsibility

Procedures: Address the Administrative for ePHI

- Address Workforce Security (Authorization, Access, Clearance & Termination)
- Access Authorization, Establishment & Modification
- Security Awareness Training
- Security Incident Procedures
- Contingency Planning
- Ensure yearly training for employees that access PHI.

Procedures: Address the Physical for (ePHI):

- Workstation Use and Security
- Device and Media Controls Disposal and Reuse
  - When destroying PHI (paper, film or other hard copy media), use a cross-cut shredder or shredding service that renders the information unreadable.
- Data backup and storage

Procedures: Address the Technical for ePHI:

- Unique User Identification
- Emergency Access Procedures
- Automatic Logoff
- Audit Controls & Integrity
- Person or Entity Authentication

Breach/Incident Response Plan

- At a minimum, name an individual to act as the investigator of the breach (e.g., privacy officer, security officer, risk manager, etc.). The investigator shall be responsible for the management of the breach investigation, completion of a risk assessment, and coordinating with others in the organization as appropriate.

  EPCC Compliance Officer: Souraya A. Hajjar, shajjar@epcc.edu

If you have a breach:

- Provide notice to the affected individual and the HHS if more than 500 affected individuals.
- For notice to the HHS, it can be immediate, or at the end of the calendar year if less than 500 affected individuals.
- Notice should contain:
  - A brief description of what happened, including dates.
  - A description of the types of unsecured PHI involved.
  - Steps the individual should take to protect against potential harm.
  - A brief description of the steps that you or your BA took to investigate the incident and mitigate harm and protect from future breaches.
  - Contact Information.

Notice to Individuals

- Generally, written notice should be made via first class mail.
  - If there is insufficient contact information for 10 or fewer individuals, substitute notice via e-mail or telephone is allowed.
  - If there is insufficient contact information for 10 or more individuals, substitute notice via a conspicuous posting on your web site, major print or major broadcast notice is allowed.
- For breaches involving more than 500 individuals, notice to the HHS must be made at the same time. If less than 500 individuals, notice to the HHS can be provided at the end of the year.
- Sample breach notification letter at http://www.ahcancal.org/facility_operations/hipaa/Documents/Sample%20Notification%20Letter%20for%20Affected%20Party.pdf.

TMPA-Texas Medical Privacy Act

TMPA is as stringent as HIPAA but for Texas medical and Dental providers. A training is required as in HIPAA and the same information is to be included. Training is required once every two years for providers. It is an exact photocopy of HIPAA..

HB 300 in Texas State legislation passed TMPA Regulation this summer and it became effective on September 1, 2012.

Since EPCC is considered a hybrid entity(School and Clinic), then we are bound to train our health care personnel, faculty and students about TMPA.

References:

- https://www.cms.gov/HIPAAGenInfo/Downloads/CoveredEntitycharts.pdf
- http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html
- http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html
- http://www.hipaa.com/2009/09/hipaa-protected-health-information-what-does-phi-include
- https://www.cms.gov/HIPAAGenInfo/Downloads/CoveredEntitycharts.pdf
- https://www.cms.gov/HIPAAGenInfo/Downloads/CoveredEntitycharts.pdf

References:

- http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf
- http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf
- http://www.ahcancal.org/facility_operations/hipaa/Documents/Sample%20Notification%20Letter%20for%20Affected%20Party.pdf

HIPAA-HITECH-TMPA

- Questions? Call Souraya A. Hajjar, EPCC Compliance Officer at 915-831-4143 or email at shajjar@epcc.edu