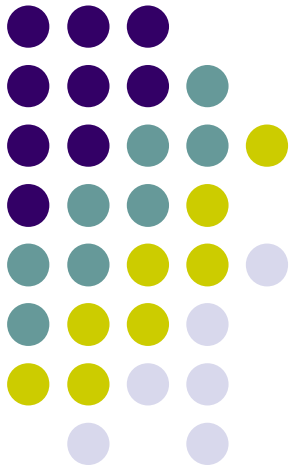
HIPAA Training

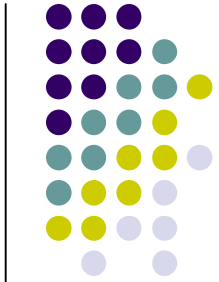
Wood County Employees Health Benefits Plan

August 21, 2013

Presented by: Pamela Boyer
HR & Benefits Manager
HIPAA Privacy Officer

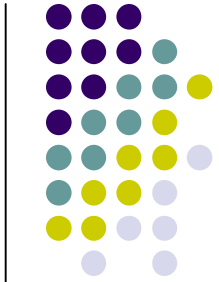


Background



- HIPAA: Health Insurance Portability and Accountability Act of 1996
- HITECH: Health Information Technology for Economic and Clinical Health Act
  - Part of the American Recovery and Reinvestment Act (ARRA) of 2009
- GINA: Genetic Information Nondiscrimination Act of 2008
  - Applies to Health Care & Employment

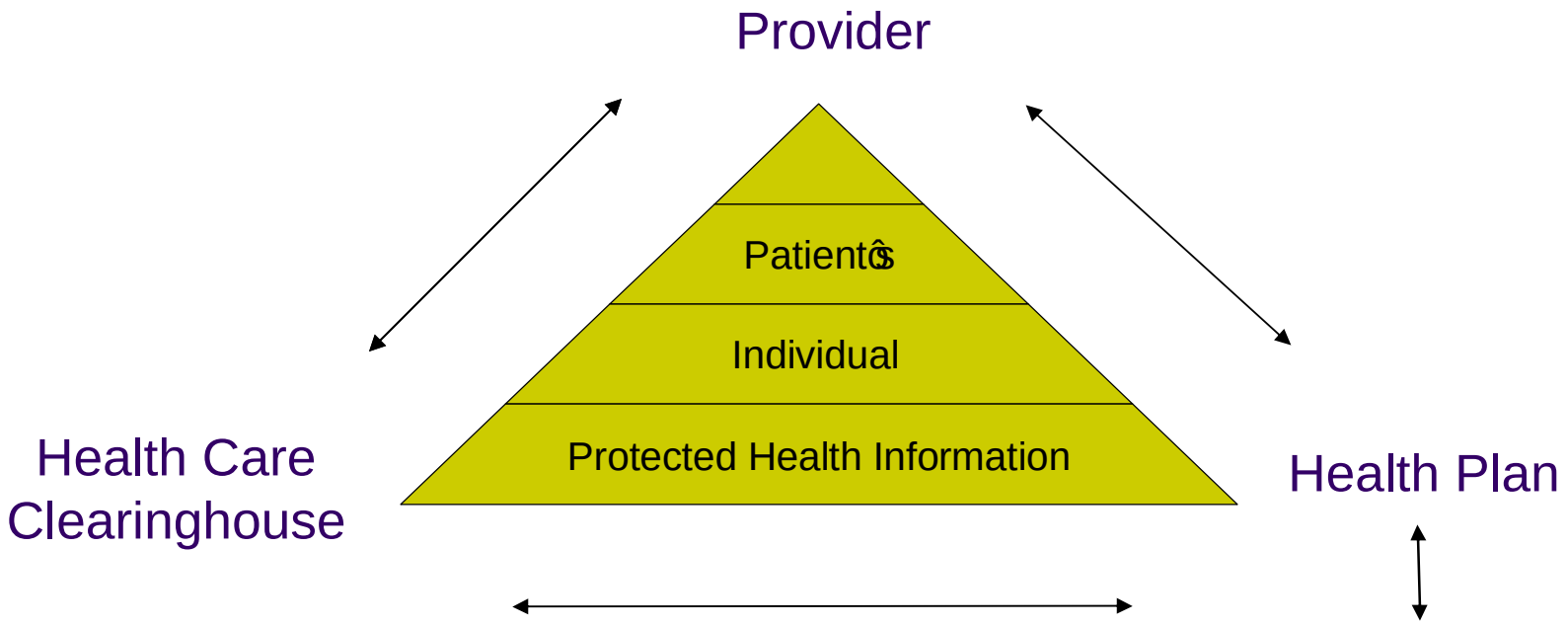
Background



- Requires Covered Entities to implement certain administrative, physical and technical safeguards to protect individualôs health information (electronic & other formats)
- Covered Entities
  - Providers who conduct covered health care transactions electronically
  - Health Plans
  - Health Care Clearinghouses

Background

Requires Covered Entities to protect an individualôs protected health information (PHI) beyond those that need it to process a claim



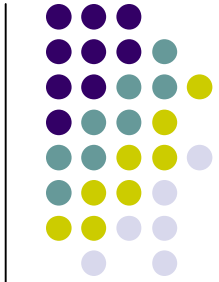
Background

- **Health information** is defined as any information whether oral or recorded in any form or medium that:
  - Is created or received by a health care provider, **health plan**, public health authority, employer life insurer, school or university, or health care clearinghouse; 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
- **Protected Health Information** means individually identifiable health information:
  - Transmitted by electronic media; maintained in electronic medial or transmitted or maintained in any other form or medium
  - Excludes: Education records covered by the Family Education Rights and Privacy Act, Employment records held by a covered entity in its role as employer

Background

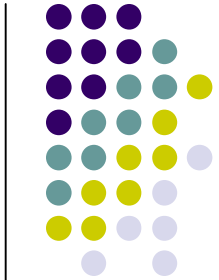
- Wood County Employees Health Benefits Plan includes the following:
  - Health care claims or equivalent encounter information;
  - Eligibility for a health plan;
  - Referral certification and authorizations;
  - Health care claim status;
  - Health plan premium payments;
  - Coordination of benefits; and,
  - Enrollment and dis-enrollment in a health plan.

Background



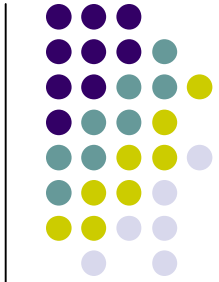
- HIPAA ONLY applies to the Wood County Employee Health Benefits Plan
- HIPAA does not apply to medical information gained in an Employer and Employee relationship
  - Request for Leave forms for use of sick leave
  - Employment records
  - FMLA
  - ADA
  - WorkersôComp
  - Other confidentiality protections may apply shielding from Public Records Requests
- Wearing of Different Hats ï Build a Wall
  - Prohibits sharing health plan information with employer

Background



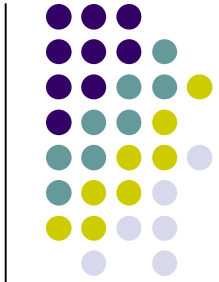
- Covered Entity must Provide Individuals with Privacy Practices, and include:
  - Explains how PHI may be used
    - TPA, treatment/payment/healthcare operations, business associates, treatment alternatives/case management, other uses (public health, abuse/neglect, law enforcement)
  - Individuals rights relative to PHI
    - Access & copy, restrictions on use & disclosure, amend, accounting, and request confidential communications
  - How to File a Complaint
    - Identify Privacy Officer: Pamela Boyer, HR & Benefits Manager
  - Provide every 3 years

Background



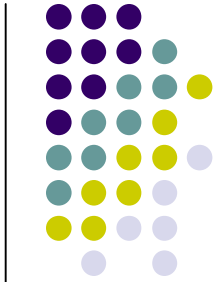
- Covered Entities must have contracts with their Business Associates to ensure compliance
  - Third Party Administrators, e.g. Meritain, PDMI, Stop Loss Vendor, Insurance Consultant
- Covered Entities (Health Plan) must provide training to staff acting on their behalf
  - Insurance Group Reps, IT, Records Center
- Requires Notification Process for Breaches in security procedures
  - Unsecured protected health information
  - Notification to individual, media, Secretary HHS
  - Maintain a log of breaches

Updated Regulations



- Final regulations issued January 25, 2013
  - Update HIPAA, HITECH and GINA
  - Effective March 26, 2013
    - Compliance Deadline: Sept. 23, 2013
    - Business Assoc Agreements: Sept. 23, 2014
- Designed to:
  - Strengthen the privacy and security protection for individualsô health information
    - Electronic formats
  - Modify the rule for Breach Notification for Unsecured Protected Health Information
  - Strengthen the privacy protections for genetic information
  - Increase flexibility for and decrease burden on the regulated entities

Four Final Rules



1. Improve the Rule:
   - Make Business Associates directly liable for compliance
   - Strengthen limitations on use and disclosure of protected info for marketing and fundraising, prohibits sale w/o individual authorization
   - Expand individualôs rights to receive electronic copies of PHI and restrict disclosures if individual paid out of pocket in full
   - Require modifications to and redistributions of Privacy Practices
   - Modify individualôs authorization for research, disclosure of child immunization proof to schools and enable access to descendent info by family members/others
   - Enhances enforcement of noncompliance with HIPAA Rules due to willful neglect

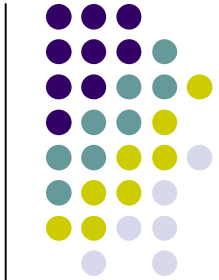
Four Final Rules

2. Increases and tiers the civil money penalty structure for non-compliance
3. Replaces the breach notification rule's õharmò threshold to more objective standard
4. Prohibits most plans from using or disclosing genetic info for underwriting

Business Associate Agreements (BAA)

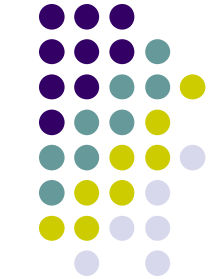
- Business Associate: creates, receives, *maintains*, or transmits protected health information on behalf of a covered entity
- Business Associates list is expanded to include:
  - Health Information Organization (HIO)
  - E-Prescribing Gateways
  - Other Persons The Facilitate Data Transmission
  - Vendors of Personal Health Records

BAA - Subcontractors



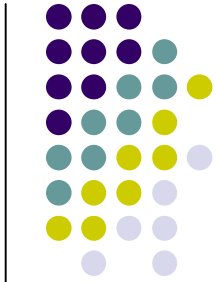
- Subcontractors
  - A person who acts on behalf of a business associate, other than in the capacity of a member of the workforce of the business associate
    - Example: Wood County (Covered Entity) has a business associate agreement with Meritain (Business Associate). Meritain hires ACME company (Subcontractor) to shred medical records on its behalf. Meritain must require that ACME comply with the privacy language in the business associate agreement with Wood County.
  - Requires updated BAA
    - BA are directly liable for their own violations under the law
    - Extend to Subcontractors
    - Revisions by 9/23/13
      - If BAA in place on 1/23/13 & not modified between 3/26/13 ï 9/23/13, law permits extension until 9/23/14

Marketing



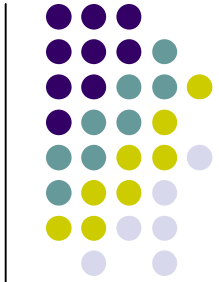
- Requires prior authorization for marketing services
  - Face to face exception
- Plan benefit information or reminders for services are exempt from definition of Marketing
  - Use of formulary
  - Refills on Prescriptions
  - Annual Mammograms

Fundraising & Sale



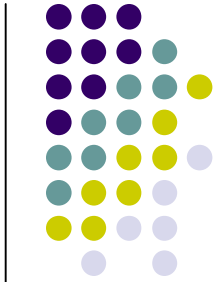
- Fundraising
  - Requires notification
  - Individual Opt out opportunities
- Sale
  - Prohibits without individual authorization

Access to PHI



- Provide in a format requested by the individual, if available
- HITECH already addresses providing information in an Electronic Health Record
  - Paper may be declined by individual if electronic available
  - Unencrypted emails may be used if individual is advised of the risk and they prefer email method
- Flexibility in future technology

Access to PHI

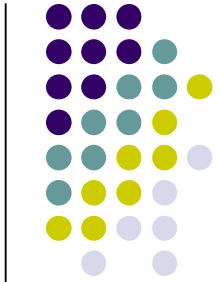


- May require the request be:
  - In writing, clear, conspicuous and specific, signed by the individual, and clearly id the designated person and where to send the copy of PHI
- May impose a reasonable, cost-based fee which includes:
  - The supplies for and labor of copying the protected health information,
  - The postage (if applicable), and
  - The preparation of an explanation or summary of PHI (if agreed to by the individual)
- Request must be timely
  - 30 day max (+ 30 days if off-site)

Notice of Privacy Practices Review

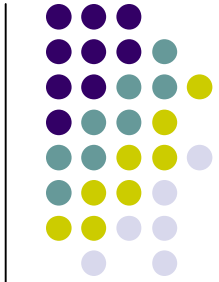
- Requires Covered Entities to have and distribute Notice of Privacy Practices (NPP)
  - Describe the uses and disclosures of PHI a covered entity is permitted to make
  - Legal duties and privacy practices with respect to PHI
  - Individualôs rights concerning PHI

Revised Notice of Privacy Practices



- Requires the Notice of Privacy Practice to Include:
  - Describe the uses and disclosures of PHI that require an authorization
    - Psychotherapy notes, PHI for marketing, sale of PHI
  - Other uses and disclosures not described in the notice will be made only with the individualôs authorization
  - Reminder appointment & fundraising Opt Out information
  - Covered Entity must agree to request to restrict disclosure of PHI to a health plan if individual paid for services out of pocket in full (only for Health Care Providers)
  - Right to be notified following a breach of unsecured PHI
- Changes are considered Material Revision

Revised Notice of Privacy Practices



- Requires Health Plan to Provide Notice to Individuals
  - Prominently post material change or its revised notice on its web site by the effective date, **and**
    - 60 days of material modification
  - Provide the revised notice, or information about the material change and how to obtain the revised notice in its next annual open enrollment period
- Distribution may use ñLayered Noticeò affect
  - Short notice if paper version available
  - Paper (email if individual agrees to electronic copy)

Revised Notice of Privacy Practices

- Requires Health Care Providers
  - First direct treatment
  - Post in prominent area for ongoing patients, paper for new

Penalties & Enforcement

- Secretary of HHS or Ohio Civil Rights may investigate
- Ongoing Audits are outsourced to a national accounting firm

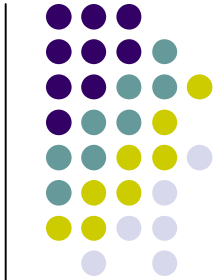
Violation Category	Each Violation	All violations of an identical provision in a calendar year
Did Not Know	$100 - $50,000	$1,500,000
Reasonable Cause	$1,000 - $50,000	$1,500,000
Willful Neglect - Corrected	$10,000 - $50,000	$1,500,000
Willful Neglect ï Not Corrected	$50,000	$1,500,000
Clearly applicable to individual employees for ñknowing misuseò	$50,000 - $250,000	1 ï 10 year

Minimum Necessary Standard Review

- Privacy Rule requires a covered entity to:
  - Make reasonable efforts to limit access to PHI to those persons who need access to carry out their duties, and
  - Disclose an amount of PHI reasonably necessary to achieve the purpose of a disclosure

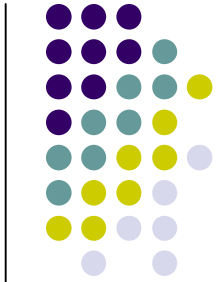
- Reminder to only share within HIPAA approved staff for Health Insurance matters only
  - Never share with Managers under any circumstances for employment related issues

Breach Notification Rule (HITECH)



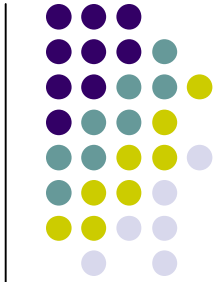
- HITECH Currently Requires
  - Covered Entities to notify the Secretary of HHS following the discovery of a breach of unsecured PHI
  - Media notification required if over 500 in state or jurisdiction
  - Business Associate (BA) to notify the Covered Entity (CE)
  - Secretary of HHS to post breaches on website involving more than 500 individuals
- Breach is an unauthorized acquisition, access, use, or disclosure of PHI which compromises the security or privacy of such info, except where an unauthorized person to whom such info is disclosed would not reasonably have been able to retain such information.
  - Disclosures where the recipient of info would not reasonably have been able to retain info
  - Certain unintentional acquisition, access or use of info by employees or other acting under the authority of a CE or BA
  - Certain inadvertent disclosures about people similarly authorized to access PHI @ CE or BA

Breach Notification Rule



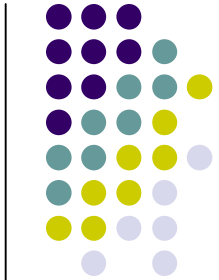
- Requires Covered Entities previous reporting requirement from ñsignificant harmòto all breaches that are not shielded from exception rule
  - Continues previous reporting requirements
  - May contractually require Business Associate to comply with Notification rule in Business Associate Agreement
  - Previous standard for immediate reporting required
- Breach is discovered on first day known or should have know by Covered Entity or BA
  - Report to Privacy Officer immediately
  - Clock starts with discovery

Breach Notification Rule



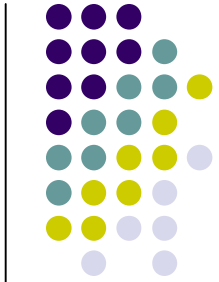
- Risk assessment must demonstrate a low probability that there is no significant risk of harm to the individual using four factors
  - Nature & extent of PHI and likelihood of re-identification
    - Financial or sensitive clinical information
  - Unauthorized person or to who the disclosure was made
    - Another entity obligated to abide by HIPAA
  - Whether PHI was actually acquired or viewed
    - Mailing vs. stolen computer never accessed
  - The extent to which the risk to the PHI has been mitigated
    - Assured that PHI is destroyed by BA vs. third party

Breach Notification Rule



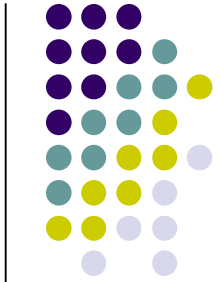
- Covered entities must provide notice to Individuals involved in the breach
  - 60 calendar days from date of discovery
  - Business Associates must notify the covered entity
- Notice to Individual shall include:
  - Description of what happened, date of breach & discovery, if known,
  - Types of unsecured PHI involved in breach,
    - Name, SSN, DOB, address, account no, diagnosis, disability code
  - Any steps to protect themselves from potential harm resulting from breach,
  - Description of covered entities steps to investigate breach, mitigate the harm to individuals and protect against any further breaches, and
  - Contact procedures to ask questions which include:
    - Toll-free number, email address, web site or postal address

Breach Notification Rule



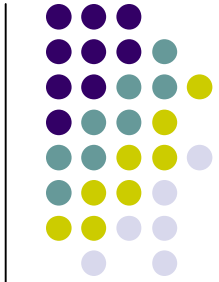
- Required to notify the Secretary HHS annually log of any breaches
  - Retain records for six years
- Unsecured PHI is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary.
  - Use of encrypting methods
- Must meet encryption and destruction consistent with National Institute of Standards and Technology (NIST)

GINA



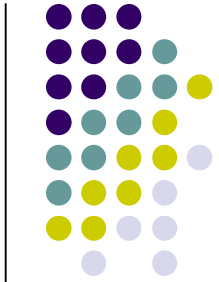
- Genetic Information Nondiscrimination Act of 2008
  - Prohibits discrimination based on an individualôs genetic information in both the health coverage (premiums) and employment context
  - Prohibits most health plans from using or disclosing genetic information for underwriting purposes
- Enforcement by DOL & HHS
  - EEOC responsible for nondiscrimination provisions based on employment

GINA



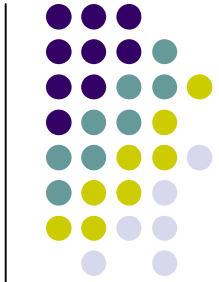
- Final Rule
  - Effective March 26, 2013, must comply by Sept. 23, 2013
  - Provides that genetic information is Health Information for the Privacy Rule
  - Prohibits health plans covered by the HIPAA Privacy Rule from using in underwriting
  - Revise provision relating to the Notice of Privacy Practices for health plans that perform underwriting based on PHI
    - Must still exclude genetic testing for rating
- Apply to Dental & Vision
  - Long term care policies excluded from law

GINA



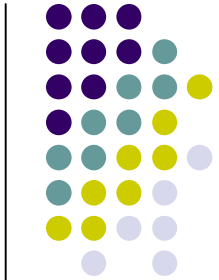
- Genetic Information
  - Genetic tests of the individual, or
  - Family health history (diseases or disorder manifested)
    - 1st, 2nd, 3rd or 4th degree relative to individual or their dependent
- Genetic Test is defined for Privacy Rule as follows
  - An analysis of human DNA, RNA, chromosomes, proteins, or metabolites that detects genotypes, mutations, or chromosomal changes
- Not Genetic Tests:
  - Medical tests or information on manifested diseases, disorders or conditions
  - HIV tests, complete blood counts, cholesterol or liver function tests, tests to detect for the presence of alcohol or drugs
  - Individual Health History Assessments as a part of wellness or disease management programs

Employer Task List



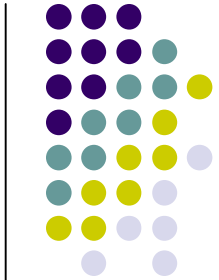
- Train relevant staff
- Update HIPAA Privacy policy & procedures
- Privacy Notice
  - Update by 9/22/13
  - Post on web by 9/23/13
  - Distribute with 2014 SPD (11/1/13) for current employees and 30 days for New Hires
- Business Associate Agreements
  - Identify business associates
  - Update agreements by 9/23/14

Administrative Staff Responsibilities



- Participate in Training
  - Use the Minimum Standard Rule
  - Never share PHI with employer
  - Notify the Plan if transferring duties
- Review Security of PHI
  - Physical: shred documents, lock drawers, keep track of who has keys, private conversations, who has access, method of collection & distribution of information
  - Technical: Screens face away from doorway, computer drive access, computer/copier vendors, secure email, routinely change secured password, lock system when not using

Administrative Staff Responsibilities



- Report PHI Breaches
  - Immediately to BCC ï same day
- Collect and Distribute PHI in a confidential manner
  - Law requires new hires receive info ï use checklist
  - Provide written privacy practices to individuals when requested
- Acknowledge Expectations by Signing
  - HIPAA Confidentiality Certification ï Confidentiality Agreement
- Direct Questions to Privacy Officer:
  - Pamela Boyer, HR & Benefits Manager