agrip
ASSOCIATION OF GOVERNMENTAL RISK POOLS

HIPAA Compliance

September 2014

Geoffrey L. Beauchamp, Esq.
General Counsel, Delaware Valley Health Trust

Petula Workman, J.D., CEBS
Division Vice President, Compliance Counsel

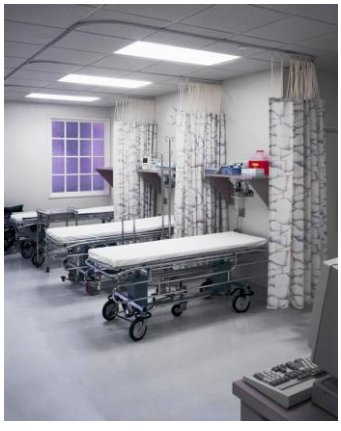
HIPAA PRIVACY, SECURITY, AND BREACH AUDITS OVERVIEW

HIPAA Privacy, Security, and Breach Audits

- The Privacy and Security Regulations were passed as part of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA")
  - Amended by the HITECH Act
- The Privacy Regulations require **"Covered Entities"** and **"Business Associates"** to follow certain rules when handling and securing certain health information called **"Protected Health Information"** (or "PHI")
- The Security Regulations establish a national set of security standards for protecting PHI held or transferred in electronic form
- The Breach Regulations address impermissible uses or disclosures under the Privacy Rule that compromise the security or privacy of PHI such that the use or disclosure poses a significant risk of financial, reputational, or other harm to an affected individual

HIPAA Privacy, Security, and Breach Audits

- **"Covered Entities"** are:
  - Health Plans
  - Health Care Clearinghouses
  - Health Care Providers
- A **"Business Associate"** is:
  - A person who, on behalf of a covered entity **such as a health plan** Uses/accesses/re-discloses PHI either:
    - To perform or assist in the performance of a plan function OR
    - To provide services to a Covered Entity



HIPAA Privacy Basics

- **"Protected Health Information" ("PHI")** is:
  - Individually identifiable health information AND
  - Created or received by a Covered Entity AND
  - Relates to
    - The past, present, or future physical or mental health of an individual; OR
    - The provision or payment for health care for an individual
- Applies to information in any format:
  - Paper
  - Electronic
  - Oral

HIPAA Privacy Basics

- Examples of PHI:
  - Enrollment information (once in the hands of the health plan)
  - List of member names, Social Security Numbers and aggregate claim dollar amount
  - List of members choosing COBRA coverage
  - E-mail with claim information for a specific member

HIPAA Privacy Basics

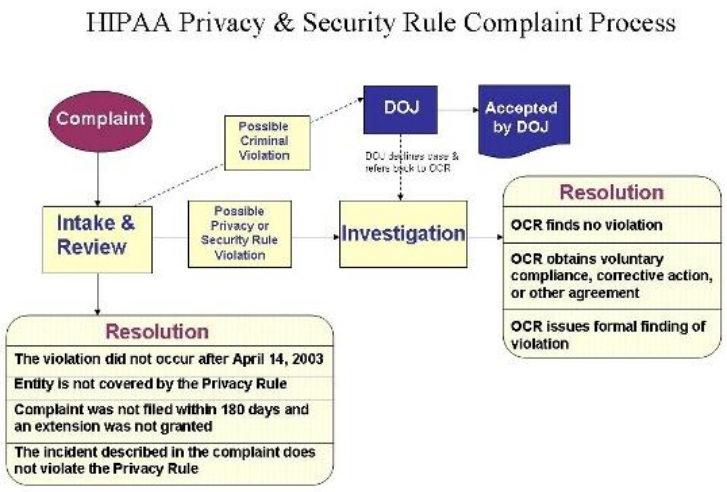
- Examples of information that is **not** PHI:
  - Enrollment information in the hands of the *employer*
  - Information kept to carry out employer's obligations under:
    - The Family & Medical Leave Act
    - The Americans with Disabilities Act
    - Similar laws
  - Records regarding:
    - Occupational injuries
    - Disability insurance eligibility
    - Fitness-for-duty exams

HIPAA Privacy, Security, and Breach Audits

- HITECH requires HHS to provide for periodic audits to ensure covered entities and business associates are complying with the HIPAA Privacy and Security Rules and Breach Notification standards
- OCR piloted a program to perform 115 audits of covered entities to assess privacy and security compliance (Phase I)
- Audits conducted during the pilot phase between November 2011 and December 2012
- New audit program for 2014 (Phase II)

8

HIPAA Privacy, Security, and Breach Audits

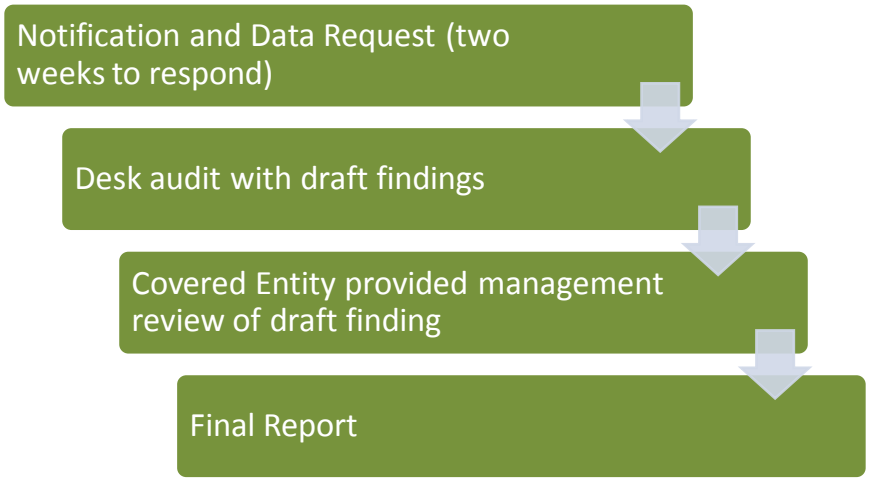


9

Phase I Audits

10

Phase II Audits



11

Phase II Audits

- New Audit Process
  - Primarily internally staffed
  - Covered entities will be asked to identify their business associates and provide current contact information
  - No on-site visits unless resources allow
  - No opportunity for investigator to seek additional information
  - Will use sampling methodology

Phase II Audits

- October 2014 through June 2015
  - 232 Providers
  - 109 Health Plans
  - 9 Clearinghouses
- OCR to use results of survey to select covered entities for audit

13

Phase II Audits

Entity Type	Privacy	Breach	Security
Covered Entities	100	100	150
• Health Plans	33	31	45
• Providers	67	65	100
• Clearinghouses	0	4	5
Business Associates	0	0	50
• IT Related	0	0	35
• Non-IT Related (e.g., TPAs, claims)	0	0	15
Total Audits by Protocol	100	100	200

14

HIPAA Privacy, Security, and Breach Audits

- Sampling of Documents Requested in Phase I
  - Demographics
  - Policies and procedures (Privacy, Security, and Breach)
  - Key person information
  - Organizational chart
  - Incident response plans
  - Risk assessment procedures
  - Contingency plans
  - System generated information (e.g., log files)
  - Technical controls information
  - Physical safeguards
  - Network diagrams
  - Notice of Privacy Practices

New HIPAA Regulations

- Omnibus regulations issued January 17, 2013
- Changes to
  - Notice of Privacy Practices
  - Policies and Procedures
    - Right to request restriction on use and disclosure
    - Right to access PHI
  - Breach Notification Rule
  - Business Associate Agreements
- GBS Technical Bulletin
  - https://ajg.adobeconnect.com/_a815130238/tb_2013_01/

Privacy

Privacy

- Administrative, Technical, and Physical safeguards
  - A covered entity must have reasonable safeguards to protect PHI from unintentional use or disclosure of PHI
  - Auditor will
    - Obtain and review written policies and procedures
    - Observe and verify that safeguards are in place and appropriate

Privacy

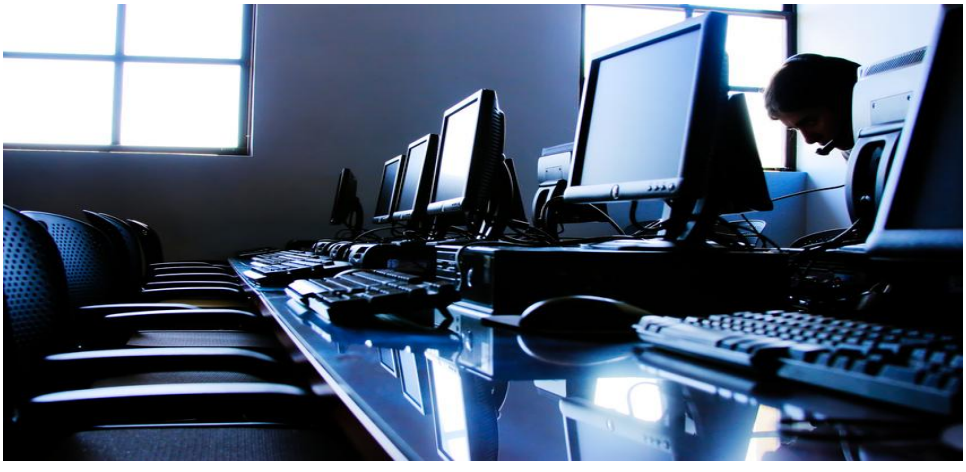
- Policies and Procedures
  - Maintaining and Updating Notice of Privacy Practices
  - Documentation of Compliance Activity
  - Limitations on Access
  - Mandatory Uses and Disclosures
  - Permissible Uses and Disclosures
  - Disclosures for Legal or Public Policy Reasons
  - Sanctions and Violations
  - Other Miscellaneous Policies

Privacy

- Mitigation
  - Covered entity must, to the extent practicable, mitigate any known harmful effect of a use or disclosure of PHI in violation of its own policies and procedures or the HIPAA regulations by itself or a business associate
  - Auditor will
    - Obtain and review policies and procedures
    - Determine if monitoring system is in place
    - Determine if policies and procedures are updated appropriately and communicated to workforce members

Privacy

- Refraining from intimidating or retaliatory acts
  - A covered entity may not intimidate, threaten, coerce, discriminate against, or take any other retaliatory action against an individual who exercises a HIPAA right or participates in the filing of a complaint either under the covered entity's own policies and procedures or with HHS
  - Auditor will
    - Obtain and review policies and procedures
    - Determine whether policies and procedures are updated appropriately and communicated to workforce members



Security

Security

- The security rule covers the administrative, technical, and physical security measures entities are required to take with regard to maintenance and transmission of electronic PHI
- Some are “required” and some are “addressable”
- The security rule applies to all electronic PHI
  - Defined as PHI that is transmitted by, or maintained in, electronic media
    - Laptops
    - Mobile devices
    - USBs
    - CDs
    - Drives
    - Desktops
    - Tablets
    - Email
  - Does not apply to paper PHI

Security

- The security rule has five categories of requirements
  1. Administrative safeguards
  2. Physical safeguards
  3. Technical safeguards
  4. Organizational requirements
  5. Policies and procedures, and documentation
- Each category has a certain number of
  - “standards”
  - each standard has “implementation specifications”, which can be “required” or “addressable”

24

Security

- "Implementation Specification: Required"
  - Entities must comply with the implementation specification
  - Unless otherwise specified, entities have flexibility in determining how best to implement the specification
    - Must take into account
      - Size, complexity, and capabilities
      - Technical infrastructure, hardware, software security
      - Probability and criticality of potential risks of ePHI compromise
      - Cost of security measures

25

Security

- "Implementation Specification: Addressable"
  - Entity must determine whether the implementation specification is a reasonable and appropriate safeguard
  - If not reasonable and appropriate, must document why it is not reasonable and appropriate
  - Entity must implement an alternative measure, again only if reasonable and appropriate
  - If an alternative measure is not implemented the entity must document why an alternative was not implemented and what measures are being done to ensure specification is being met

26

Security

- Assignment of Security Official (Required)
  - An entity must assign a security officer
  - Responsible for the development, implementation, monitoring, and communication of security policies and procedures
  - Must be a person, not a committee or group

Security

- Assignment of Security Official (Required)
  - Auditor will
    - Request information to demonstrate designation of Security Official
    - Obtain and review Security Official's assigned duties
      - E.g., a job description
    - Determine if responsibilities have been clearly defined

Security

- Conduct periodic risk analysis (Required)
  - Must have policies and procedures to conduct an accurate assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI
    - Identify all assets and information systems that create, receive, transmit, or maintain ePHI
      - Assets: Computers, mobile devices, tablets, USB, etc.
      - Information systems: Software systems

Security

- Conduct periodic risk analysis (Required)
  - Auditor will review relevant documents and content to determine:
    - If periodic risk assessment conducted
    - Whether all assets and information systems that contain, process, or transmit ePHI have been identified
    - Whether risk assessment processes have been updated to reflect any changes in organizational environment
      - E.g., new email system, new servers

Security

- At the core of a risk analysis are the following questions:
  - Have you identified the e-PHI within your organization? This includes e-PHI that you create, receive, maintain or transmit.
  - What are the external sources of e-PHI? For example, do vendors or consultants create, receive, maintain or transmit e-PHI?
  - What are the human, natural, and environmental threats to information systems that contain e-PHI?

31

Security

- Development of policies and procedures for acquisition of IT Systems and Services (Required)
  - Must have processes in place for the selection of IT systems and services that include consideration for the following:
    - Applicability of the IT solution to the intended environment
    - The sensitivity of the data
    - The organization's security policies, procedures, and standards
    - Other requirements such as resources available for operations, maintenance, and training

Security

- Development of policies and procedures for acquisition of IT Systems and Services (Required)
  - Auditor will
    - Review written policies and procedures for compliance
    - Determine whether policies and procedures are approved and updated on a periodic basis

Security

- Information System Activity Review (Required)
  - Entity must implement procedures for regular reviewing of information system activity
    - Audit logs, access reports, security incident reports
    - Sign in/out reports, what reports were accessed, denied access or gained access
  - Timing is up to the entity

Security

- Information System Activity Review (Required)
  - Auditor will
    - Review policies and procedures
    - Obtain sample of implementation of review practices (e.g., sample audit logs or access reports)
    - Determine if policies and procedures are approved and updated on periodic basis

Security

- Implementation of risk management program (Required)
  - Entity is required to implement proper security measures to reduce the risk of security threats
  - This is based on the risk analysis

Security

- Implementation of risk management program (Required)
  - Auditor will
    - Review security policies and evaluate whether security measures are sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with regulations
      - Vulnerability is defined as *"[a] flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy"*
      - Risk is defined as *"[t]he net mission impact considering (1) the probability that a particular [threat] will exercise (accidentally trigger or intentionally exploit) a particular [vulnerability] and (2) the resulting impact if this should occur . . ."*

Security

- Implementation of risk management program (Required)
  - Auditor will
    - Determine if policy is reviewed and approved on a periodic basis
    - Determine if security standard addresses data moved within the organization and data sent out of the organization

Security

- Implementation of procedures for authorization and/or supervision of workforce members (Addressable)
  - Personnel accessing ePHI must be given authorization or be supervised
  - Up to the entity to determine best way to implement
  - Must address how to keep people who do not have access from inadvertent access

Security

- Implementation of policies and procedures to ensure appropriate access to ePHI by establishing clear job descriptions and responsibilities (Addressable)
  - Auditor will
    - Obtain and review formal documentation of policies and procedures to determine level of access granted based on business need
    - If entity has determined not to fully implement this standard, obtain documentation for areas without full implementation and rationale for not fully implementing

Security

- Implementation of policies and procedures to ensure appropriate access to ePHI by establishing criteria for hiring and assigning tasks (Addressable)
  - Process to determine whether a person should have access to ePHI
  - Assessment of risk, cost, benefit, and feasibility, and any other protective measures

Security

- Implementation of policies and procedures to ensure appropriate access to ePHI by establishing criteria for hiring and assigning tasks (Addressable)
  - Auditor will
    - Obtain and review documentation demonstrating that staff members have necessary knowledge, skills, and abilities to fulfill particular roles
    - Obtain and review documentation that management verified the required experience and qualifications per management policy
    - If entity has determined not to fully implement this standard, obtain documentation for areas without full implementation and rationale for not fully implementing

Security

- Establishment of Workforce Clearance (Addressable)
  - Process to determine whether a person should have access to ePHI
  - Assessment of risk, cost, benefit, and feasibility, and any other protective measures

Security

- Establishment of Workforce Clearance (Addressable)
  - Auditor will
    - Obtain and review policies and procedures
    - Obtain and review evidence of approval or verification of access to ePHI
    - If entity has determined not to fully implement this standard, obtain documentation for areas without full implementation and rationale for not fully implementing

Breach Notification

Breach Notification

- What is a "breach"?
  - An unauthorized acquisition, access, or use or disclosure of unsecured protected health information in a manner not permitted by the HIPAA Breach regulations which compromises the security or privacy of such information
    - "Unsecured" means that the information was not destroyed or otherwise rendered unusable (e.g., encrypted)
    - Not every disclosure is a breach
    - There are exceptions, but that is beyond the scope of our discussion today

Breach Notification

- Risk Assessment of Breach
  - Breach means the acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Breach Notification regulations that compromises the security or privacy of the PHI
  - Auditor will
    - Ask if risk assessment process exists to determine whether breach exists
  - Should have written policies and procedures

Breach Notification

- Notice to Individuals
  - A covered entity is required to notify each impacted individual whose unsecured PHI has been or is reasonably believed to have been used, accessed, acquired, or disclosed as a result of a breach
  - Auditor will
    - Obtain and review key documents that outline the process for notifying individuals of breaches
  - Should have model forms to use to track investigation and notify individuals, HHS, and the media of breaches

Breach Notification

- Timeliness of Notification
  - A covered entity is required to provide notice of a breach without unreasonable delay, but in no case later than 60 days after the discovery of the breach
  - Auditor will
    - Obtain and review key documents that outline the process for notifying individuals
    - Verify timing of breach notification, if any have occurred

Breach Notification

- Methods of Individual Notification
  - Written notification is required, but if individual is deceased, notification may be given to next of kin or personal representative
  - Auditor will
    - Obtain and review documents that provide methods for notifying individuals and compare to actual performance
    - Request process to identify contact information or next of kin and the process to follow up if insufficient contact information
    - Obtain and review documents that provide methods to provide notice when contact information is insufficient or out-of-date

Breach Notification

- Content of Notification
  - Notification must contain
    - Brief description of what occurred
    - Date of breach
    - Date of discovery of breach (if known)
    - Description of unsecured PHI that was involved (e.g., Social Security number, diagnosis, etc.)
    - Steps individual should take to protect himself or herself from potential harm (e.g., notification of credit agencies)
    - Description of what covered entity is doing to investigate, mitigate harm, and protect against future potential breaches
    - Contact procedures for questions or additional information (e.g., toll free number to call)

Breach Notification

- Content of Notification
  - Auditor will
    - Determine if any standard template or form letter used for breach notification
    - Verify notifications sent to individuals contained required elements, if any breaches occurred

agrip
ASSOCIATION OF GOVERNMENTAL RISK POOLS

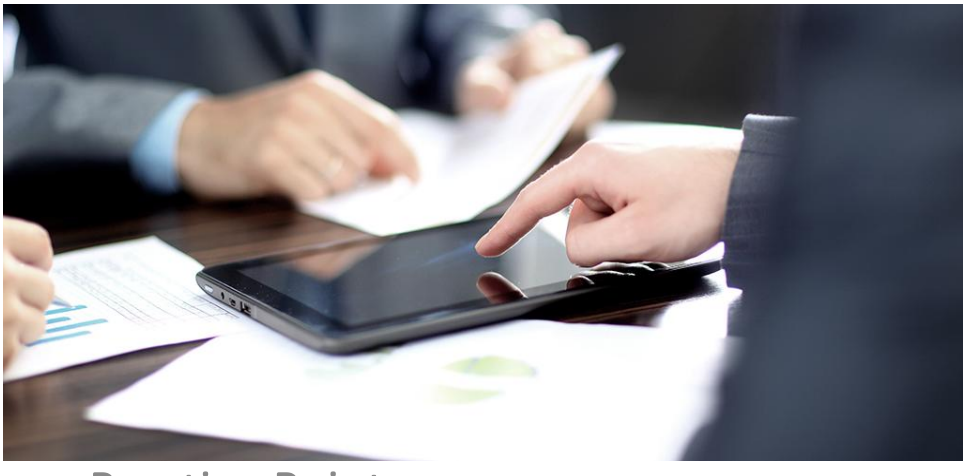
Impact on Health Pools and their Participants

Impact on Health Pools and their Participants

- Role of pools and their participants in HIPAA compliance
- Pools and pool participants as HIPAA “covered entities” and “business associates”
- Pools and pool participants as “plan sponsors” and “controlling health plans”

Impact on Health Pools and their Participants

- Handling PHI
  - The enrollment process
  - COBRA administration
  - Wellness programs
  - Coverage appeals
  - Claims handling and benefit plan inquiries
  - Large claims data
- Security requirements and IT infrastructure



Practice Pointers

Practice Pointers

- Audit Focus (Round 1)
  - Security
    - Risk analysis and risk management
  - Breach
    - Content and timeliness of notifications
  - Privacy
    - Notice and Access
- Audit Focus (Round 2) (Projected for 2015)
  - Security
    - Device and media controls, transmission security
  - Privacy
    - Safeguards, training to policies and procedures
- Audit Focus (Round 3) (Projected for 2016)
  - Security
    - Encryption and decryption; physical facility access control; other areas of high risk identified in 2014 audits; and breach reports and complaints

57

Practice Pointers

- Have pre-response strategy call with consultants
- Obtain advice of legal counsel when situation difficult
- Prepare documents in tabbed and labeled binders
- Consider vendor documents and procedures
- Prepare narrative responses in consultation with consultants and/or legal advisors
- Make sure that individuals required for interviews are available (if on-site visit occurs)
- Treat auditors with courtesy

HIPAA Privacy, Security and Breach Audits

- Resources
  - OCR Privacy & Security Audit webpage
    - http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html
  - OCR Privacy Assistance
    - http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/privacyguidance.html
  - OCR Security Assistance
    - http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html

Questions & Answers

The intent of this presentation is to provide you with general information regarding the topic presented. It does not necessarily fully address specific issues with respect to your employee benefits environment. It should not be construed as, nor is it intended to provide, legal advice. Questions regarding specific issues should be addressed by your general counsel or an attorney who specializes in this practice area.

60

Thank You

Geoffrey L Beauchamp, Esq.
General Counsel
Delaware Valley Health Trust
267.803.5715 Phone
267.803.5765 Fax
gbeauchamp@dvit.com

Petula Workman, J.D., CEBS
Division Vice President,
Compliance Counsel
Arthur J. Gallagher & Co.
713.358.5856 Phone
713.358.5857 Fax
petula_workman@ajg.com