HIPAA Privacy and Security for Employers

Cottingham & Butler

Wednesday, January 10, 2018

Benefit Comply

Employee Benefit Compliance Support

Presented By:

Sarah Grcevich

Consultant,

Benefit Comply

Alana Kenyon

Consultant,

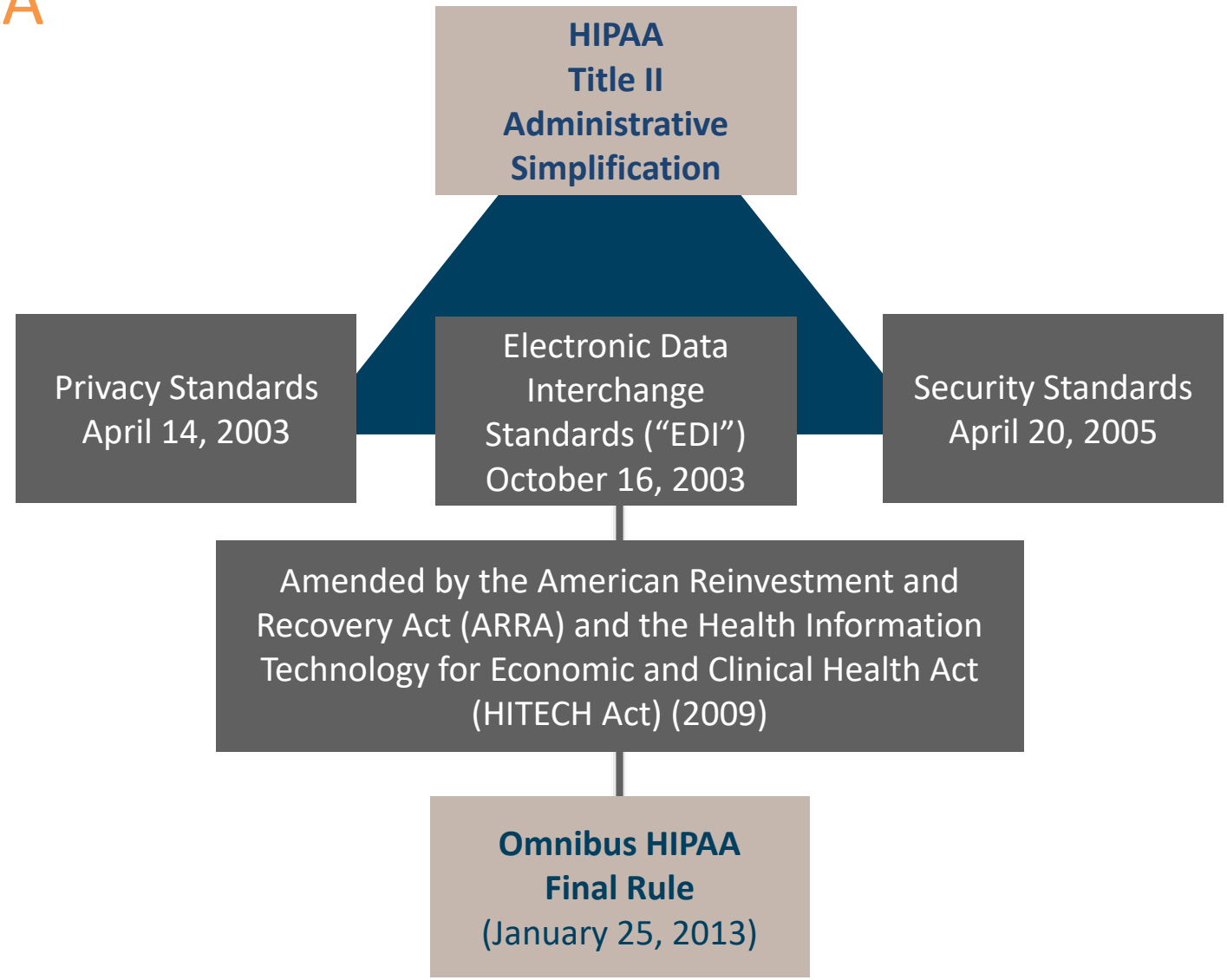
Benefit Comply

Agenda

- HIPAA Background/Overview
- Who Has to Comply
- Some Common Misperceptions
- Overview of HIPAA Privacy and Security Rules
- What Employers Need to Do
- Why Does it Matter (Enforcement, Audits)
- Summary – What Employers Need to Do
- We Can Help

HIPAA Overview/Background

HIPAA


HIPAA
Title II
Administrative
Simplification
Privacy Standards
April 14, 2003
Electronic Data
Interchange
Standards ("EDI")
October 16, 2003
Security Standards
April 20, 2005
Amended by the American Reinvestment and Recovery Act (ARRA) and the Health Information Technology for Economic and Clinical Health Act (HITECH Act) (2009)
Omnibus HIPAA
Final Rule
(January 25, 2013)

Who Has to Comply?

HIPAA Applicability

- HIPAA applies to all "Covered Entities," including:
  - Health Care Providers
  - Health Care Clearinghouses
  - Health Plans
    - Health Plans offered by Insurance Companies
    - Employer-sponsored health plans (e.g., medical, dental, prescription, vision, health FSAs, EAPs, wellness, HRAs)
- Plans not subject to HIPAA:
  - Disability, Worker's Compensation, HSAs
- HIPAA applies to Business Associates

HIPAA Applicability

- Employer/Plan Sponsor versus Group Health Plan
  - They are separate legal entities!
  - The Group Health Plan is Covered Entity, Subject to HIPAA
    - No employees
  - Employer/Plan Sponsor is not a Covered Entity, but it is responsible for overseeing and ensuring the health plan's compliance with HIPAA.

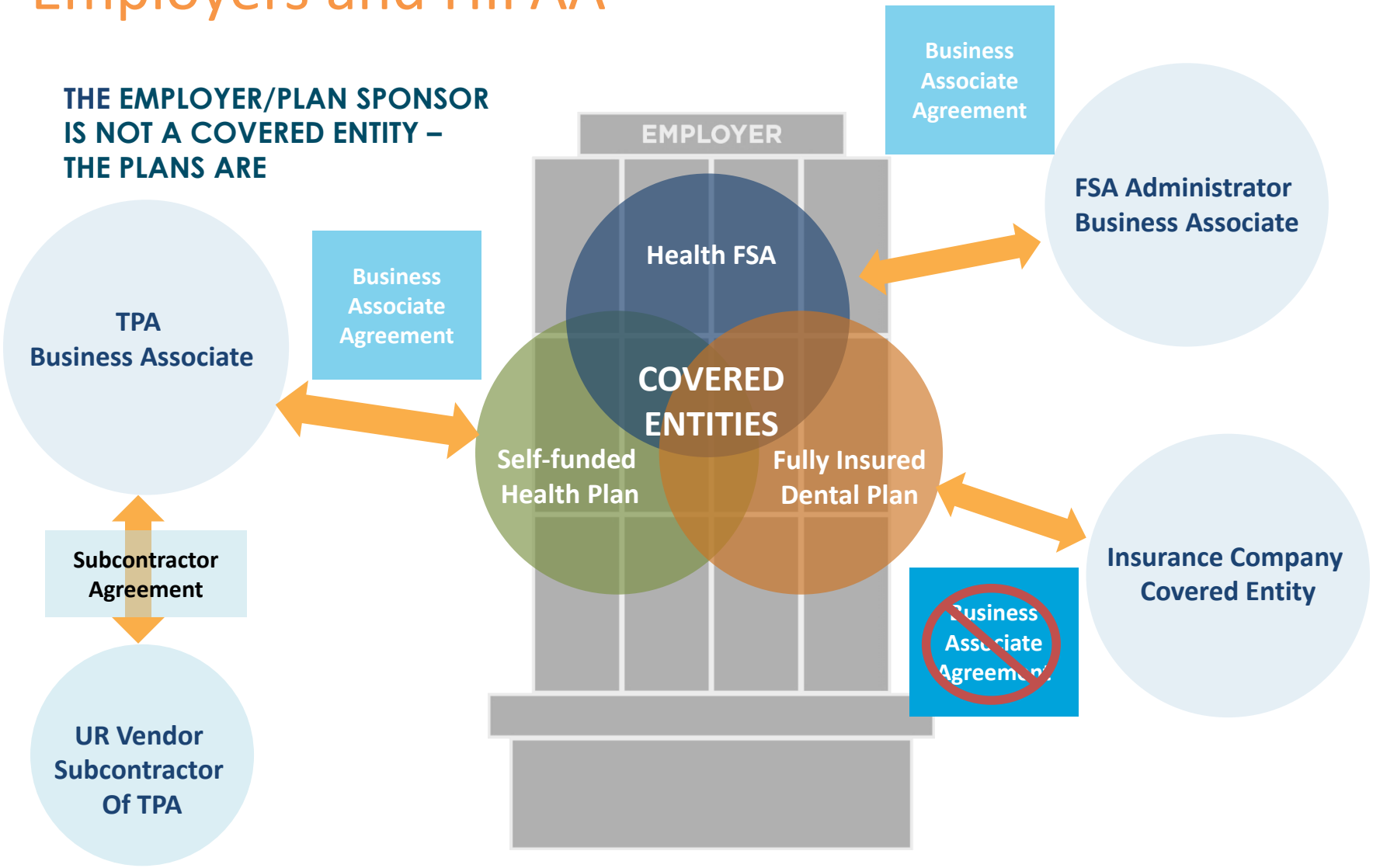
Employers and HIPAA

- Fully Insured Plans
  - Both the employer health plan and the insurance carrier are HIPAA Covered Entities
    - No Business Associate Agreement needed between employer and carrier
- Self-Funded Employer Plans
  - Employer-sponsored self-funded health plans are always HIPAA Covered Entities
    - Includes Section 125 Health FSAs and HRAs
    - Employer cannot avoid HIPAA requirements simply by telling TPA not to share PHI with employer
    - TPA is a Business Associate, not a Covered Entity

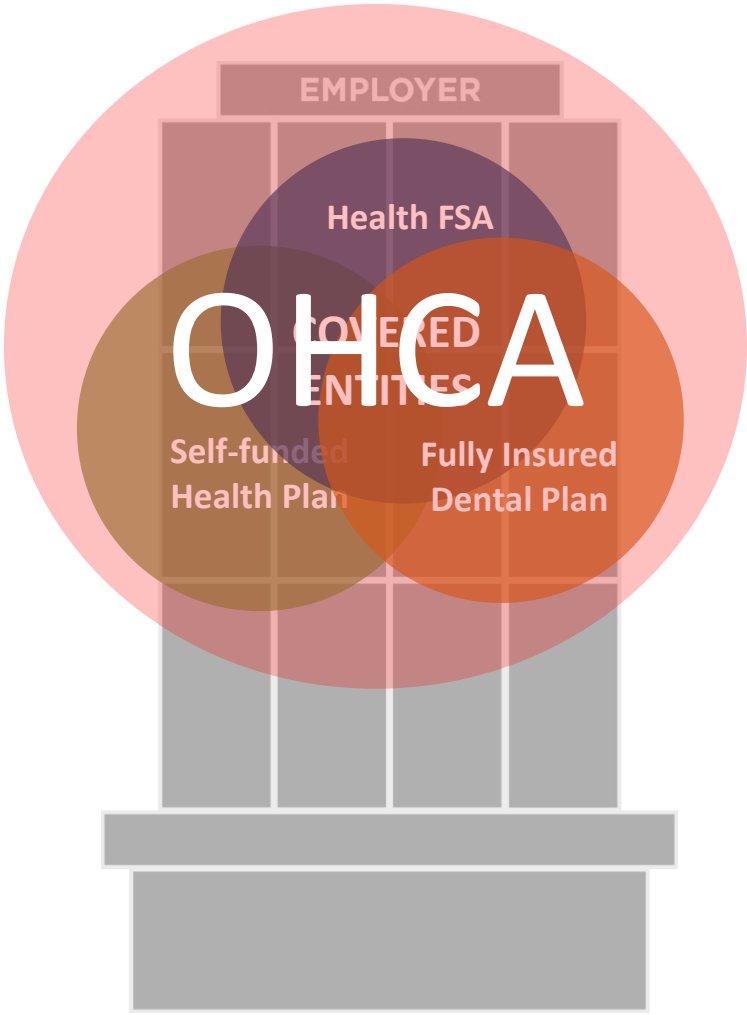
Employers and HIPAA

- Access to PHI
  - "Level 1" (Fully Insured only)
    - Access only "Summary Health Information" & Enrollment/Disenrollment Data
    - Limited privacy and security obligations
  - "Level 2" (Fully Insured or Self-funded)
    - Access to PHI beyond Summary Health Information & Enrollment/Disenrollment Data
    - Must certify HIPAA compliance to plan before can release PHI
    - Privacy and security requirements apply (but limited obligations for Notice of Privacy Practices if fully insured).

Employers and HIPAA



- Organized Health Care Arrangement (OHCA)
  - A plan sponsor may treat all plans subject to HIPAA as a single OHCA
    - One set of policies and procedures
    - One Notice of privacy practices
    - One privacy and security official
    - etc.



Employers and HIPAA

- Common Employer Misperceptions
  - All I need to do is send a Notice of Privacy Practices
  - My insurance company sends a privacy notice so I don't have to
  - All I need to do is have my employees attend HIPAA training
  - I am fully-insured so I don't have to do anything
  - I am a small employer so HIPAA does not apply to me

HIPAA Privacy Rules

HIPAA Privacy Requirements

1. Organized Health Care Arrangement
2. Privacy Official
3. Policies and Procedures
4. Group Health Plan
5. Health Plan Identifier Number
6. Uses and Disclosures
7. Minimum Necessary
8. Authorizations
9. Personal Representatives
10. Business Associates
11. Limited Data Set
12. De-Identification
13. Notice of Privacy Practices
14. Safeguards
15. Breaches
16. Complaints
17. Access
18. Accounting
19. Amendments
20. Confidential Communication
21. Restrictions
22. Workforce Training
23. Sanctions & Mitigation

What is Protected Health Information (PHI)?

- PHI
  - Individually identifiable Information relating to physical or mental health of an individual
  - Created, maintained or transmitted by a Covered Entity
    - For our purposes, this means the information must be related to the employer sponsored health plan
- Other Employee Medical Information – NOT PHI
  - Employers have access to other confidential employee information not subject to HIPAA
  - Americans With Disabilities (ADA) confidentiality rule
  - State Laws

HIPAA Privacy Rule

- HIPAA restricts the use of PHI
  - To certain uses allowed by the law
  - To times when the individual gives a specific written authorization to use the information
- Uses allowed without an individual's authorization
  - Treatment, Payment & Health Care Operations (TPO)
    - For our purposes this means that the plan can use PHI for legitimate plan administration purposes, but other uses are strictly limited
  - Other uses allowed without an individual's authorization
    - Required by law, public health, etc.

Use and Disclosure of PHI Issues

- Areas Where HIPAA Commonly Impacts Employers
  - Employers Use of PHI for Other Purposes
    - PHI may not be used by employer for employment related activities unless the individual specifically authorizes the use (e.g. Job related physicals, FMLA, ADA)
  - Limiting other employee access to PHI
    - Does the CFO need identity specific health information???
  - Disclosures about and to spouses or adult children
    - Restrictions on what can be disclosed to spouse
      - Limited to that individual's own information unless there is an authorization
    - Additional information can be disclosed to "subscriber"
      - Reimbursement related information (EOBs example)

Use and Disclosure of PHI Issues

- Areas Where HIPAA Commonly Impacts Employers (Cont.)
  - The Privacy Notice
    - Plans must send notice of privacy practices (NPP) to all participants
      - Many employers depend on carrier to send NPP for fully-insured plans – however you should review carrier's NPP
      - Carrier NPP may not be applicable to employer's plan
      - Plan sponsors may want to create on NPP for an OHCA
    - A reminder that the NPP is available must be sent at least every 3 years

HIPAA Security Rules

HIPAA Security Rules

- Security Standards and Implementation Specifications
  - The Security Rule contains 22 standards that must be addressed
    - Administrative Safeguards
    - Physical Safeguards
    - Technical Safeguards
    - Organizational, Policies and Procedures and Documentation Requirements
- Security Risk Analysis
    - Employers required to conduct a HIPAA security risk analysis
- Security measures are appropriate and reasonable
  - Considerations - Size, complexity, mission, purposes of ePHI created, maintained, sent and received…..

Standards	Sections	Implementation Specifications (R)= Required, (A)=Addressable	
Security Management Process	164.308(a)(1)	Risk Analysis	(R)
		Risk Management	(R)
		Sanction Policy	(R)
		Information System Activity Review	(R)
Assigned Security Responsibility	164.308(a)(2)		(R)
Workforce Security	164.308(a)(3)	Authorization and/or Supervision	(A)
		Workforce Clearance Procedure	(A)
		Termination Procedures	(A)
Information Access Management	164.308(a)(4)	Isolating Health care Clearinghouse Function	(R)
		Access Authorization	(A)
		Access Establishment and Modification	(A)
Security Awareness and Training	164.308(a)(5)	Security Reminders	(A)
		Protection from Malicious Software	(A)
		Log-in Monitoring	(A)
		Password Management	(A)
Security Incident Procedures	164.308(a)(6)	Response and Reporting	(R)
Contingency Plan	164.308(a)(7)	Data Backup Plan	(R)
		Disaster Recovery Plan	(R)
		Emergency Mode Operation Plan	(R)
		Testing and Revision Procedure	(A)
		Applications and Data Criticality Analysis	(A)
Evaluation	164.308(a)(8)		(R)
Business Associate Contracts and Other Arrangement	164.308(b)(1)	Written Contract or Other Arrangement	(R)

Facility Access Controls	164.310(a)(1)	Contingency Operations	(A)
		Facility Security Plan	(A)
		Access Control and Validation Procedures	(A)
		Maintenance Records	(A)
Workstation Use	164.310(b)		(R)
Workstation Security	164.310(c)		(R)
Device and Media Controls	164.310(d)(1)	Disposal	(R)
		Media Re-use	(R)
		Accountability	(A)
		Data Backup and Storage	(A)

Access Control	164.312(a)(1)	Unique User Identification	(R)
		Emergency Access Procedure	(R)
		Automatic Logoff	(A)
		Encryption and Decryption	(A)
Audit Controls	164.312(b)		(R)
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information	(A)
Person or Entity Authentication	164.312(d)		(R)
Transmission Security	164.312(e)(1)	Integrity Controls	(A)
		Encryption	(A)

Business Associate Contract or other arrangement	164.314(a)(1)	Business Associate Contracts	(R)
		Other Arrangements	(R)
Requirements for Group Health Plans	164.314(b)(1)	Implementation Specifications	(R)

Policies and Procedures	164.316(a)		(R)
Requirements for Group Health Plans	164.316(b)(1)	Time Limit	(R)
		Availability	
		Updates	(R)

What Employers Need to Do

Employers and HIPAA

- Employer HIPAA Compliance Checklist
  - **Privacy**
    - Designate Privacy Official
    - Establish written HIPAA policies and procedures to address requirements spelled out in the rules (appropriate use and disclosure, limited access, physical safeguards, etc.)
    - Develop policies to address a HIPAA breach
  - **Security**
    - Designate Security Official
    - Conduct security risk assessment
    - Establish written HIPAA policies and procedures to address requirements in the rules (securing data, access rights, etc.)
    - Make sure corporate IT training includes required HIPAA security reminders
  - **General**
    - Create/update plan documents, notice of privacy and other documents
    - Identify business associates (BA) and update BA agreements
    - Develop sanctions for employees who violate HIPAA policies
    - Provide HIPAA training for employees who handle PHI

Why It Matters

HIPAA Enforcement

- HIPAA enforced by Department of Health and Human Services Office of Civil Rights (OCR)
  - Enforcement historically complaint driven
    - Privacy notices have HHS contact information
    - HHS has a website where individuals can report violations
- HITECH increased enforcement of HIPAA
  - HHS required to conduct periodic compliance audits
  - Penalties collected will be used to finance additional enforcement
  - Significant increase in potential penalties

HIPAA Enforcement (Cont.)

- OCR HIPAA Compliance Audits Phase II
  - HHS has published a detailed description of Phase II Audit Protocol
    - http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html
  - HHS protocol document includes description of what auditors will be looking for – Here are a few examples:
    - *"Obtain and review policies and procedures regarding uses and disclosures. Evaluate whether the uses and disclosures of PHI are consistent with the entity's notice of privacy practices."*
    - *"Does the covered entity enter into business associate contracts as required? Do these contracts contain all required elements? Obtain and review policies and procedures related to the identification of business associates and the creation and establishment of business associate agreements."*
    - *"Obtain and evaluate group health plan documents to determine if they restrict the use and disclosure of PHI to the plan sponsor"*

HIPAA Privacy & Security Penalties

HIPAA Violations	Penalties	
Civil Penalties	**Each Violation**	**All violations of an identical provision in a calendar year**
Due to unknowing violation	$112 - $55,910	$1,677,299
Due to reasonable cause but not willful neglect	$1,118 - $55,910	$1,677,299
Due to willful neglect that is timely corrected	$11,182 - $55,910	$1,677,299
Due to willful neglect not timely corrected	$55,910 -$1,677,299	$1,677,299
Criminal Penalties	**Fines**	**Imprisonment**
Clearly applicable to individual employees (not just the entity) – for “knowing misuse”	$50,000 - $250,000	1-10 years

To Wrap Up – What Employers Need To Do

- Employer HIPAA Compliance Checklist
  - **Privacy**
    - Designate Privacy Official
    - Establish written HIPAA policies and procedures to address requirements spelled out in the rules (appropriate use and disclosure, limited access, physical safeguards, etc.)
    - Develop policies to address a HIPAA breach
  - **Security**
    - Designate Security Official
    - Conduct security risk assessment
    - Establish written HIPAA policies and procedures to address requirements in the rules (securing data, access rights, etc.)
    - Make sure corporate IT training includes required HIPAA security reminders
  - **General**
    - Create/update plan documents, notice of privacy and other documents
    - Identify business associates (BA) and update BA agreements
    - Develop sanctions for employees who violate HIPAA policies
    - Provide HIPAA training for employees who handle PHI

Benefit Comply

Employee Benefit Compliance Support

Compliance Services

	Assurex Global Partner Firm	Benefit Comply Retainer Client
HIPAA GUARDIAN *Consultant-Driven Compliance Project* Our consultant takes care of the entire process for the employer by conducting a multi-phase project that includes performing a risk analysis, developing policy and procedures, training staff, and more to ensure that the client is in compliance with the HIPAA Privacy and Security Rules.	$6,500	$5,500
HIPAA SHIELD *Compliance Software* The employer drives their own process with the help of our proprietary HIPAA Compliance Web Tool, which provides all the resources they need to achieve compliance with the HIPAA Privacy and Security Rules.	$995	$795
NEW! HIPAA SHIELD PLUS *Compliance Software Plus Unlimited Consultant Access* The employer uses our proprietary HIPAA Compliance Web Tool to fulfill their HIPAA compliance requirements on a self-service basis, but also has unlimited phone and email access to our HIPAA consultants, who will answer questions and assist in completing the process.	$2,900	$2,500
NEW! HIPAA HERO WORKSHOP *Multi-employer Workshop* Become a HIPAA HERO and sponsor a day-long HIPAA workshop for employers. In the workshop, a Benefit Comply consultant will engage directly with a small group of employers to help them work through the HIPAA compliance process. Attendees will leave the workshop with much of what they need to do already completed and an understanding of any additional steps they need to take to fulfill their HIPAA compliance obligations.		

Compliance Services

Deliverables Comparison	HIPAA Guardian	HIPAA Shield Plus	HIPAA Shield
One-on-one kick-off call	✓		
Consultant-led security risk analysis	✓		
Consultant-drafted privacy and security policy creation	✓		
Consultant-led, in-depth policy review with client	✓		
Live staff training (onsite or web based)	✓		
Access to HIPAA Helpline	✓	✓	
Recorded staff training module library	✓	✓	
Sample documents (e.g. BA agreement, Notice of Privacy Practices, etc.)	✓	✓	✓
Web-based privacy and security policy templates		✓	✓
Template risk analysis		✓	✓
Explanatory Articles and resources		✓	✓
Staff training guide		✓	✓