Compliancy Group
Achieve.Illustrate.Maintain.
Compliance Simplified

HIPAA 101 for Eye Care:

The Guide to Understanding and Solving HIPAA Compliance

855 85 HIPAA (855-854-4722)
www.CompliancyGroup.com

Compliancy Group

We simplify compliance so you can confidently focus on your business.

Started in 2005 by HIPAA auditors & Compliance experts

- Market need for a total end client solution
- Created **The Guard**: cloud-based solution

Compliance is our business

- **No client has ever failed an OCR or CMS audit!**
- 100% of our clients would refer us to a friend
- **Recognized Leader** of Compliance
  - Top Compliance Tools & Emerging Vendor

Endorsed by

- **AOAExcel, PERC, Vision Trends, iDoc, First Eye Care**
- **iMatrix, Ocuco, Coherent Eye, Eyetopia**
- Plus 40 other medical associations and technology providers – hosting, EHR, IT, Security

HHS Wall of Shame

Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
Massachusetts Eye and Ear Infirmary	MA	Healthcare Provider	1076	01/08/2010	Theft	Other
Children's Eyewear Sight	CA	Healthcare Provider	1080	01/12/2015	Theft	Desktop Computer
Eye Institute of Corpus Christi	TX	Healthcare Provider	43961	02/26/2016	Theft	Electronic Medical Record
EyeCare of Bartlesville	OK	Healthcare Provider	4000	03/13/2015	Hacking/IT Incident	Desktop Computer, Network Server
Massachusetts Eye and Ear Infirmary	MA	Healthcare Provider	3594	04/20/2010	Theft	Laptop
Oakland Vision Services, PC	MI	Healthcare Provider	3000	05/03/2012	Hacking/IT Incident	Network Server
Southeast Eye Institute, P.A. dba eye Associates of Pinellas	FL	Healthcare Provider	87314	05/05/2016	Hacking/IT Incident	Network Server
University of Houston for UH College of Optometry	TX	Healthcare Provider	7000	05/08/2012	Hacking/IT Incident, Unauthorized Access/Disclosure	Network Server
Silicon Valley Eyecare Optometry and Contact Lenses	CA	Healthcare Provider	40000	05/13/2010	Theft	Network Server
Associates in EyeCare, P.S.C.	KY	Healthcare Provider	971	05/16/2016	Theft	Laptop, Other Portable Electronic Device
Gulf Breeze Family Eyecare, Inc	FL	Healthcare Provider	9626	06/17/2013	Theft, Unauthorized Access/Disclosure	Desktop Computer, Electronic Medical Record, Email, Network Server, Paper/Films
Cefalu Eye-Tech of Green, Inc.	OH	Healthcare Provider	850	07/14/2016	Unauthorized Access/Disclosure	Electronic Medical Record
Ferris State University - MI College of Optometry	MI	Healthcare Provider	3947	10/11/2013	Hacking/IT Incident	Network Server
Envisionfx	OH	Business Associate	540	10/23/2015	Unauthorized Access/Disclosure	Paper/Films
Indiana University School of Optometry	IN	Healthcare Provider	757	10/25/2011	Theft	Network Server
Visioneworks Inc.	TX	Health Plan	74944	11/10/2014	Loss	Network Server
REEVE-WOODS EYE CENTER	GA	Healthcare Provider	30000	11/15/2014	Theft	Network Server
Visioneworks Inc.	TX	Health Plan	47683	11/21/2014	Theft	Network Server
True Vision Eyecare	OH	Healthcare Provider	542	11/21/2014	Theft	Laptop
Robbins Eye Center PC	CT	Healthcare Provider	1749	11/26/2012	Theft	Desktop Computer

Based on HHS Breach Portal: Breaches Affecting 500 or More Individuals, "Type of Breach" https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

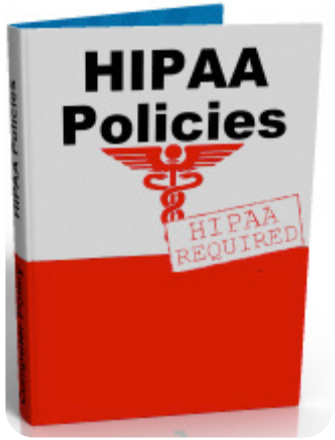
Are YOU HIPAA Compliant?

We are HIPAA compliant…

Risk Assessments

- I had an expensive Security Risk Assessment done
- Am I HIPAA compliant?

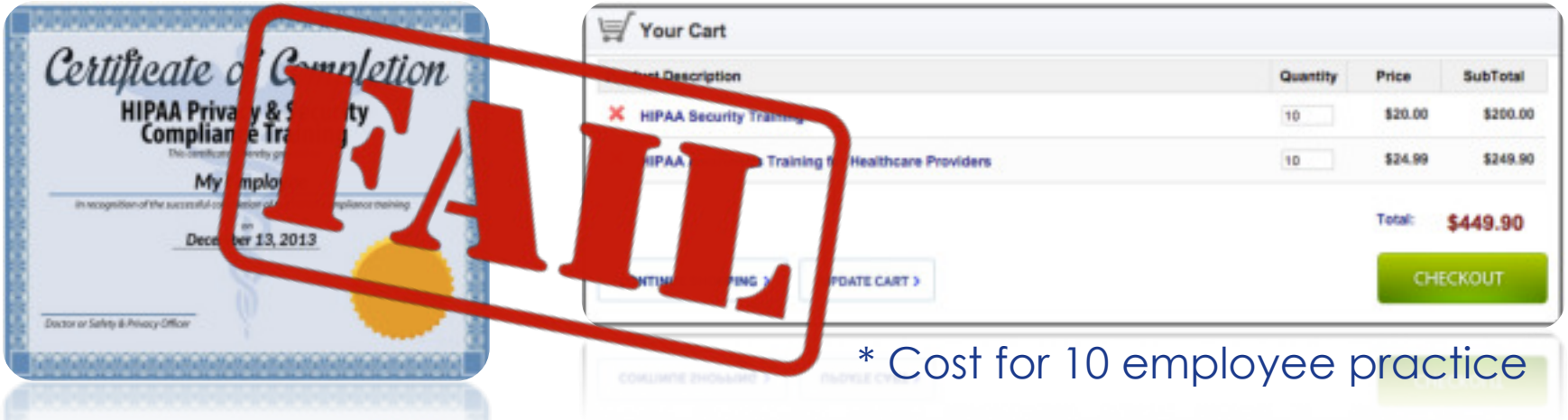
Policies & Procedures



- I have a Manual, I am compliant "right"?

Workforce Training

- I paid for my employees HIPAA training, I am compliant.

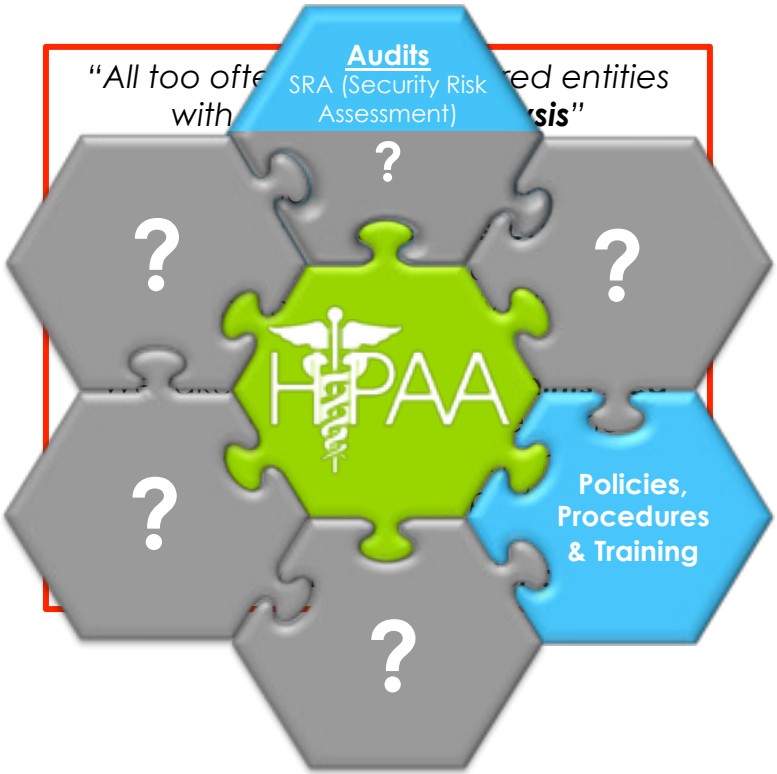


* Cost for 10 employee practice

Why Should I Worry About HIPAA?

HIPAA is the Law

- **Current market solutions often only address *pieces* of compliance**
- **Enforcement is on the rise ↑** 400%
  - Record fines levied:
    - **$9.3 Million** in 2014
    - **$6.2 Million** in 2015
    - **$24 Million** in 2016
    - **$16.7 Million** so far in 2017*
  - Three prison sentences
  - Medical license revoked
  - State Attorney General levying fines



http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html

Avoidable Breach

- Who: Anchorage Community Mental Health Services (ACMHS) - **Nonprofit** org. **(Alaska)**
- What: **Malware** caused breach of unsecured ePHI
- Why:
  - *Audits*
  - *Policies & Procedures*
  - *Training*
- Settlement: **$150,000 & CAP (Corrective Action Plan)**

Important Definitions

Covered Entity (CE): Health care providers, health plans, health care clearinghouses who electronically transmit any Protected Health Information (PHI)

Business Associate (BA): Any individual or organization that creates, receives, maintains or transmits PHI on behalf of a Covered Entity (CE)

Subcontractor: Create, receive, maintain or transmit PHI on behalf of a BA

What Information Does HIPAA Protect?

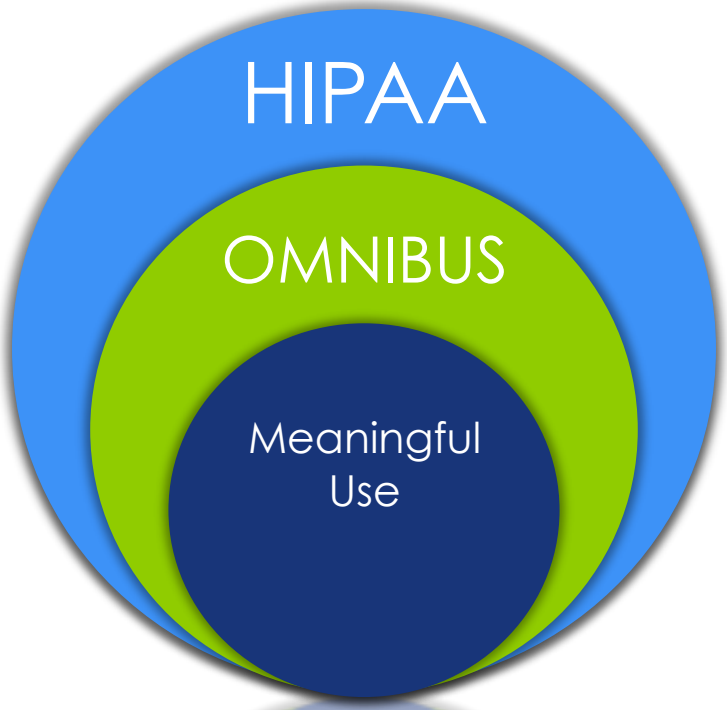
PHI may include any of the following:

- Names
- Addresses
- Dates of Service
- Telephone Numbers
- Fax Numbers
- Email Addresses
- Social Security Numbers
- Medical Record Numbers
- Health Plan Beneficiary Numbers

- Account Numbers
- Certificate/License Numbers
- Vehicle identifiers/Serial Numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers;
- Biometric identifiers
- Full Face Photos or Videos
- Any other unique identifying number, characteristic, or code

What is HIPAA Compliance and what is NOT

- **Compliance vs. Security**
  - Fines vs. Risk
- **HIPAA/HITECH**
  - Protect patient confidentiality while furthering innovation and patient care
  - Privacy Rule and Security Rule
- **Omnibus**
  - Business Associates must be HIPAA compliant
  - Covered Entities must have BAAs
    - Conduct Due Diligence
  - Breach Notification Rule
- **Meaningful Use**
  - Accelerate adoption of EHR (electronic Health records)



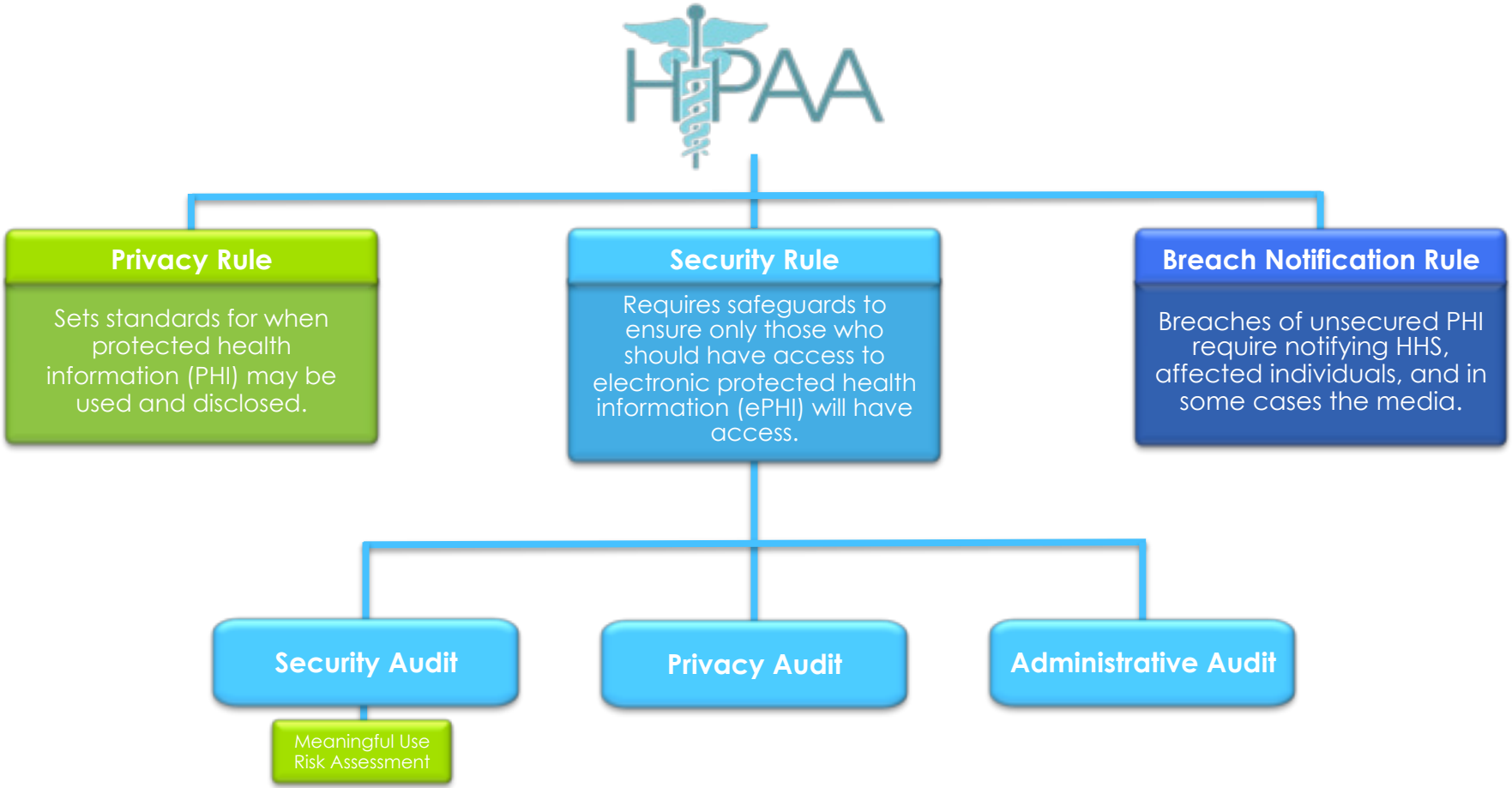
Compliance vs. Security

- Audits
  - Security, Privacy, and Administrative
- Gap Identification
- Remediation
- Policies & Procedures
- Employee Training & Attestation
- Business Associate Management
  - BA Agreements & Audit
- Incident Management

- Security Risk Analysis
- Penetration Testing
- Remediation
  - Vulnerability Scan
- Prevention
  - System Hardening
- Detection
  - Behavioral monitoring
  - Network Security Monitoring

Security Risk Assessment

FINES → **REPUTATION** ← RISK



Omnibus Rule

- Business Associates:
  - Direct liability by function
  - Directly liable for violations
  - Must be HIPAA Compliant (Security Rule)
    - **Technical**, **Administrative, & Physical** Safeguards
- Covered Entities:
  - Compliance with Privacy Rule
  - Must have BAAs (Business Associate Agreements)
  - Conduct **Due Diligence**
  - for the CE
- Contracting with subcontractors
  - BA liability flows to all subcontractors

"I heard the new HIPAA Omnibus Rules are a whole lot tougher on business associates."

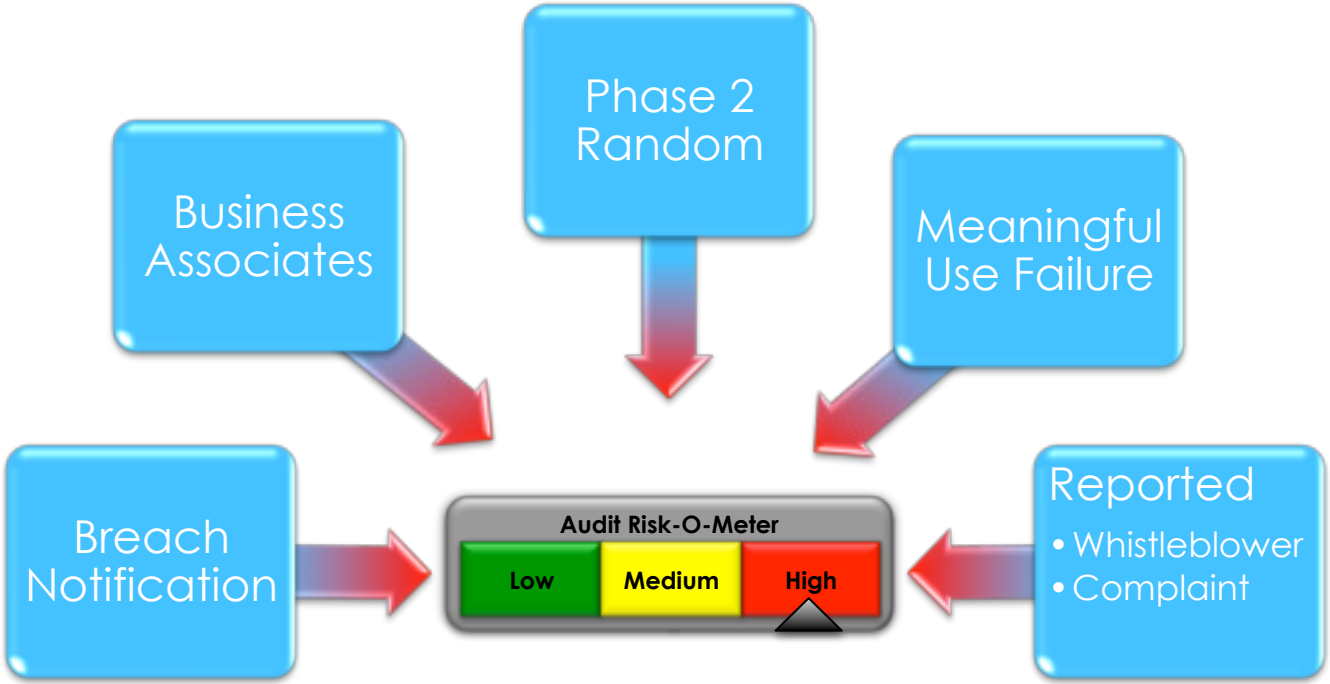
The Seven Fundamental Elements of an Effective Compliance Program

Compliance according to HHS:

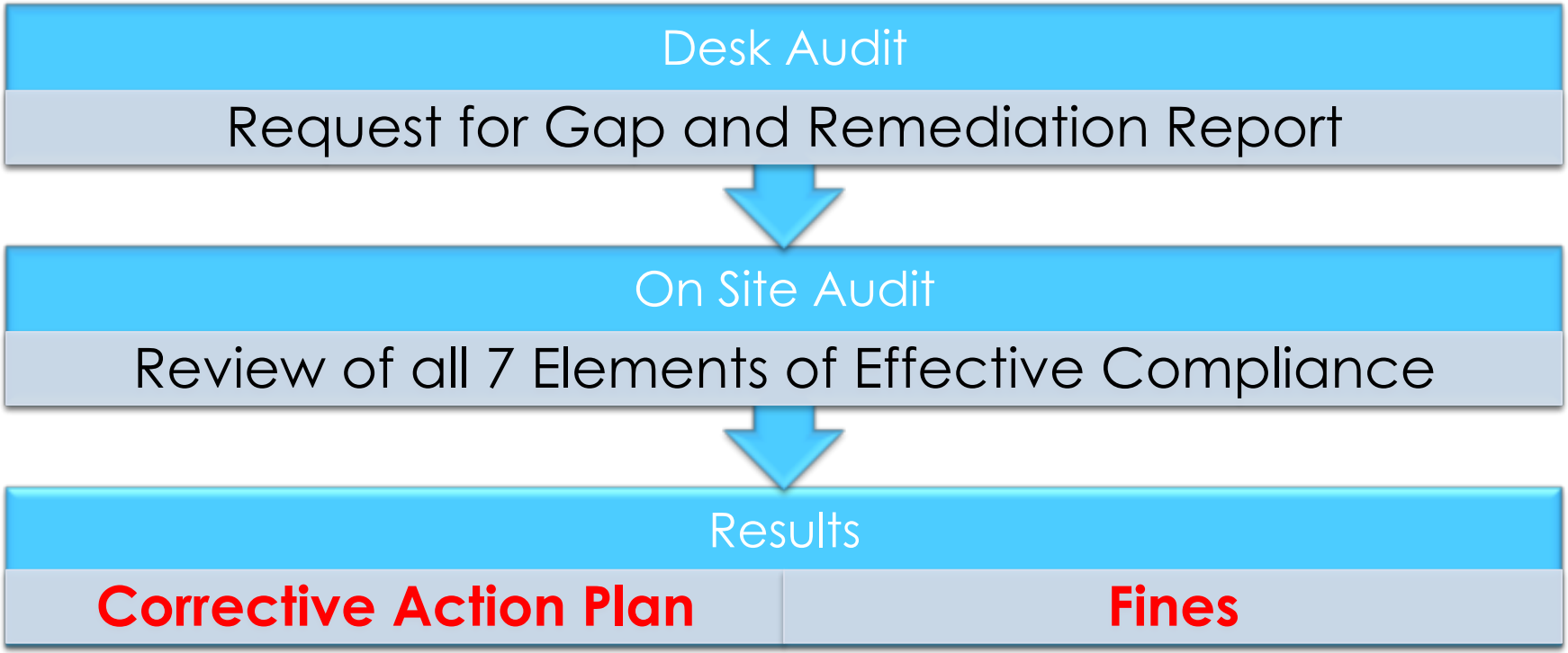
1. *Implementing written policies, procedures and standards of conduct.*
2. *Designating a compliance officer and compliance committee.*
3. *Conducting effective training and education.*
4. *Developing effective lines of communication.*
5. *Conducting internal monitoring and auditing.*
6. *Enforcing standards through well-publicized disciplinary guidelines.*
7. *Responding promptly to detected offenses and undertaking corrective action.*

*Source HHS & OIG

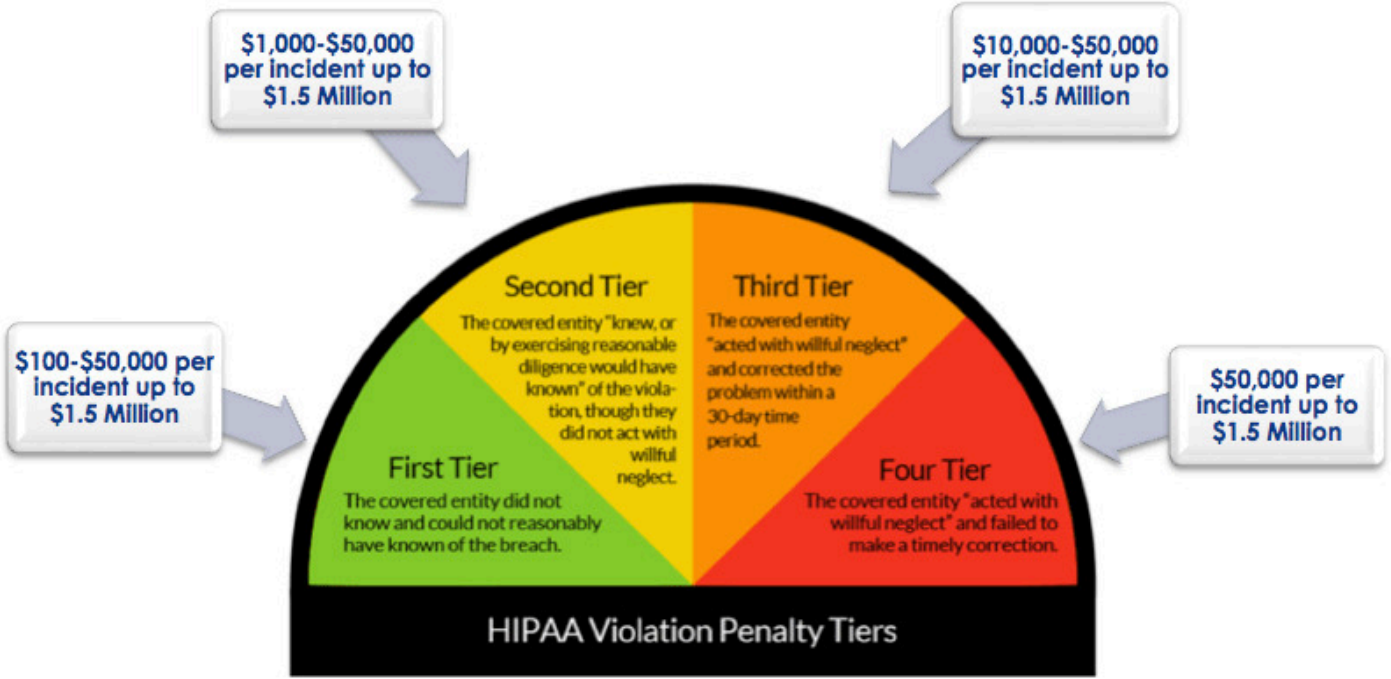
Causes Of A HIPAA Audit



The Process Of An Audit



Penalties



The Need For BAAs

- Who: Raleigh Orthopaedic (North Carolina)
- What/Why: 17,300 patients affected
  - Handed over PHI to potential business partner without first executing a **business associate agreement**.
- Settlement: **$750,000 & CAP** (4/20/16)

"HIPAA's obligation on covered entities to obtain **business associate agreements** is more than a mere check-the-box paperwork exercise," said **Jocelyn Samuels, Director of OCR**. "It is critical for entities to know to whom they are handing PHI and to obtain assurances that the information will be protected."

http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/raleigh-orthopaedic-clinic-bulletin/index.html

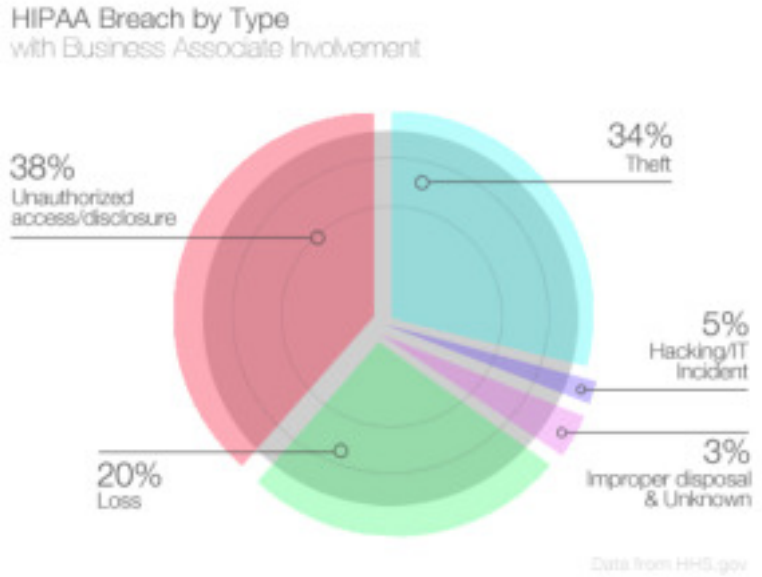
$31,000 Mistake

- Who: The Center for Children's Digestive Health (CCDH), **small pediatric practice**
- What: **Investigation of a BA (Filefax)**
- Why:
  - Caused by OCR investigating improper disposal of PHI by Filefax;
  - Subsequent investigation detected lack of BAA with CCDH
- Settlement: **$31,000 & CAP** (4/20/17)

https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/ccdh/index.html

But…It Probably Won't Happen To Me

- In a recent study, **more than half** of business associates (**59%**) reported a data breach in the last two years that involved the loss or theft of patient data. More than a quarter (**29%**) experienced two breaches or more.
- Of the 345 incidents reported by HHS and listed on their site under Breaches Affecting 500 or More Individuals, 74 involved a business associate (**21%**).



Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data conducted by Ponemon Institute
http://media.scmagazine.com/documents/121/healthcare_privacy_security_be_30019.pdf

Lack of Timely Breach Notification = **$475k**

- Who: Presence Health
- What/Why: 836 patients affected
  - Breach: missing paper operating room schedules
  - **Failed to notify within 60 days** each of the 836 individuals affected
  - **Failed to notify OCR within 60 days**
- Settlement: **$475,000 & CAP** (1/9/17)

"Covered entities need to have a clear policy and procedures in place to respond to the **Breach Notification Rule's timeliness requirements**" said OCR Director Jocelyn Samuels. "Individuals need **prompt notice of a breach** of their unsecured PHI so they can take action that could help mitigate any potential harm caused by the breach."

https://www.hhs.gov/about/news/2017/01/09/first-hipaa-enforcement-action-lack-timely-breach-notification-settles-475000.html

Solving The HIPAA Compliance Puzzle

Compliancy Group

We simplify compliance so you can confidently focus on your business.

The Guard

- Total HIPAA compliance Solution
- Simple & Cost-Effective
- **Achieve, Illustrate and Maintain™** methodology
  - **No client has ever Failed an Audit!**
- Compliance Support
  - Compliance Coaches
  - HIPAA Hotline, Email, chat or call
  - Breach Support & Audit Support
- Seal of Compliance
  - Verification and Validation of your HIPAA compliance
- **Vision Trend Members – 3 Months Free**

Questions? Need Help with Compliance?

Marc Haskelson
President & CEO
855-854-4722 Ext 507
Marc@compliancygroup.com

VISION TRENDS

855 85 HIPAA Ext 517
(855-854-4722) Ext 517
www.CompliancyGroup.com
info@compliancygroup.com