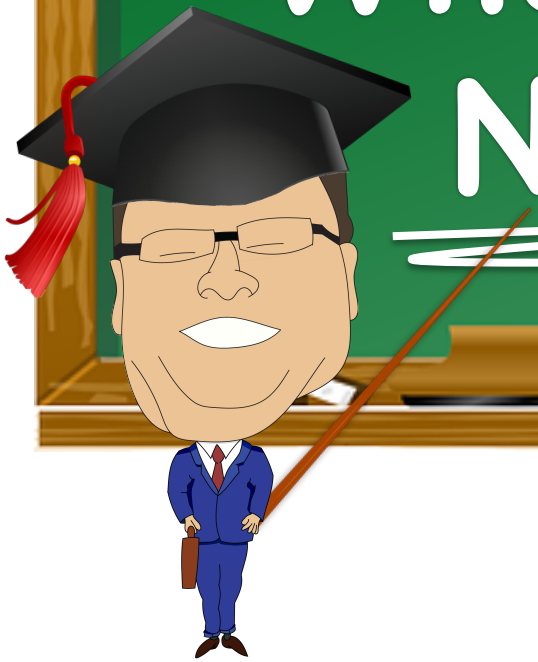
HIPAA 101: What All Doctors NEED To Know



Compliancy Group
Achieve.Illustrate.Maintain.
Compliance Simplified

HIPAA Basics

- HIPAA: Health Insurance and Portability Accountability Act of 1996
- Purpose: to **protect** confidential information through improved security and privacy standards

The HIPAA Privacy Rule

- The HIPAA privacy rule defines the type of information that must be kept private by categorizing it as "**Protected Health Information**," or PHI for short.
- PHI can exist in written, oral, and electronic formats

Compliancy Group
Achieve.Illustrate.Maintain.
Compliance Simplified

Examples of PHI

- Name
- Birth Date
- Fax Number
- Account Number
- Web Universal Resource Locator (URL)
- Street Address
- Admission Date
- Electronic mail address
- Certificate/License Number
- License Plate Number
- City
- Discharge Date
- Social Security Number

- Vehicle and Serial Number
- Device Identifier and Serial Number
- Precinct
- Date of Death
- Medical Record Number
- Internet Protocol Number
- Full Face Photographic Images
- Zip Code
- Telephone Number
- Health Plan Beneficiary Number
- Biometrics Identifiers (i.e. finger prints)
- Any Other Unique Identifying Number, Characteristic, or Code

Compliancy Group
Achieve.Illustrate.Maintain.
Compliance Simplified

Minimum Necessary

- Limits the way Workforce Members may use and disclose PHI. The **workforce must have a job-related reason to use and/or disclose PHI.**
- Requires that the workforce use only the **minimum amount** of PHI necessary to get the job done. This is what HIPAA defines as the **MINIMUM NECESSARY** Standard.
- Our Workforce: an employee, contracted provider, volunteer, trainee, subcontractor, consultant or other under direct supervision.

Patient Privacy Rights

- Right to access PHI
- Right to request an amendment to PHI
- Right to request restrictions on how PHI is used for treatment, payment, and healthcare operations
- Right to receive confidential communications
- Right to request an accounting of disclosures
- Right to complain to the Department of Health and Human Services' Office for Civil Rights

HIPAA Security

- HIPAA security applies to **PHYSICAL**, **TECHNICAL**, and **ADMINISTRATIVE** safeguards that are put in place to protect the confidentiality of information.

Passwords

ID Numbers

File Cabinets

Protected Information

Compliancy Group
Achieve.Illustrate.Maintain.
Compliance Simplified

Electronic Protected Health Information

- HIPAA requires administrative, physical, and technical safeguards to be implemented to address the confidentiality, integrity, and availability of **ELECTRONIC PROTECTED HEALTH INFORMATION (ePHI).**

Compliancy Group
Achieve.Illustrate.Maintain.
Compliance Simplified

HIPAA Compliance

HIPAA compliance

- Mandatory for 7,000,0000 Covered Entities (CE) & Business Associates (BA)
- 70% of the market is **NOT** compliant!

HITECH/EHR incentive requires:

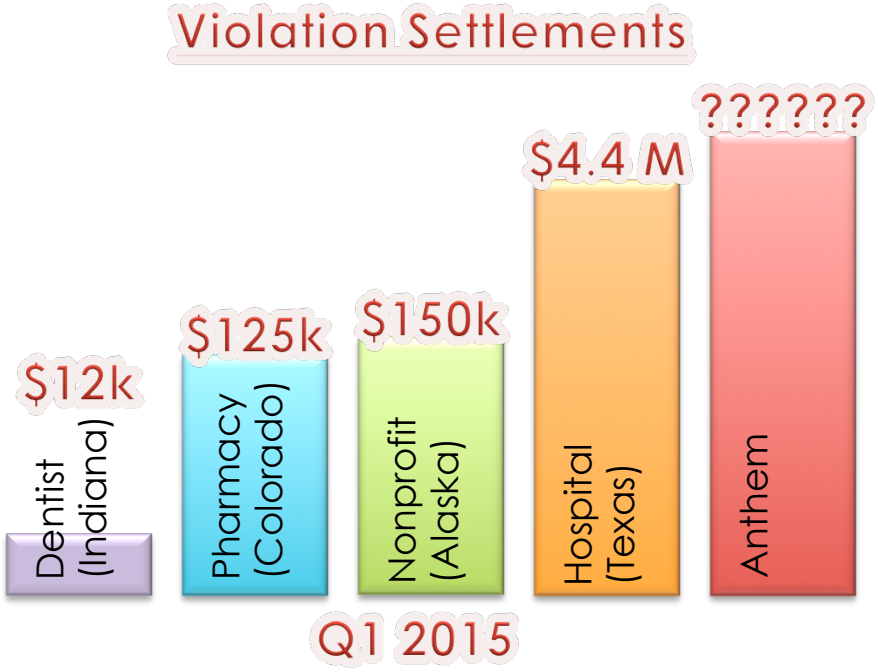
- Stage 1. Risk Assessment for Meaningful Use Core Measure 15
- Stage 2. Illustrate corrective actions

Omnibus Rule

- Compliance date was September 2013
- Requires CEs/BAs to be HIPAA compliant
- CE must have (BAAs) Business Associate Agreements

Trends in HIPAA Enforcement

1 in 4 Americans  Affected by Anthem Breach



- Indiana Dentist – License Permanently Revoked for **"Mishandling medical records"**
- Denver Pharmacy – ***" failed to provide training as required by the Privacy Rule."***
- Alaskan Nonprofit – ***"policies and procedures were not followed and/or updated."***
- Wellpoint Inc. – ***$1.7 Million settlement caused by a BA performing software upgrade***

Compliancy Group
Achieve.Illustrate.Maintain.
Compliance Simplified

The Big Misconception

"I completed a Risk Assessment, I'm HIPAA Compliant."

A Risk Assessment is only a part of HIPAA compliance.

ALL aspects of HIPAA are needed to pass an audit.

- **70%** of Covered Entities are not compliant
- **79%** of Covered Entities fail their Meaningful Use audit

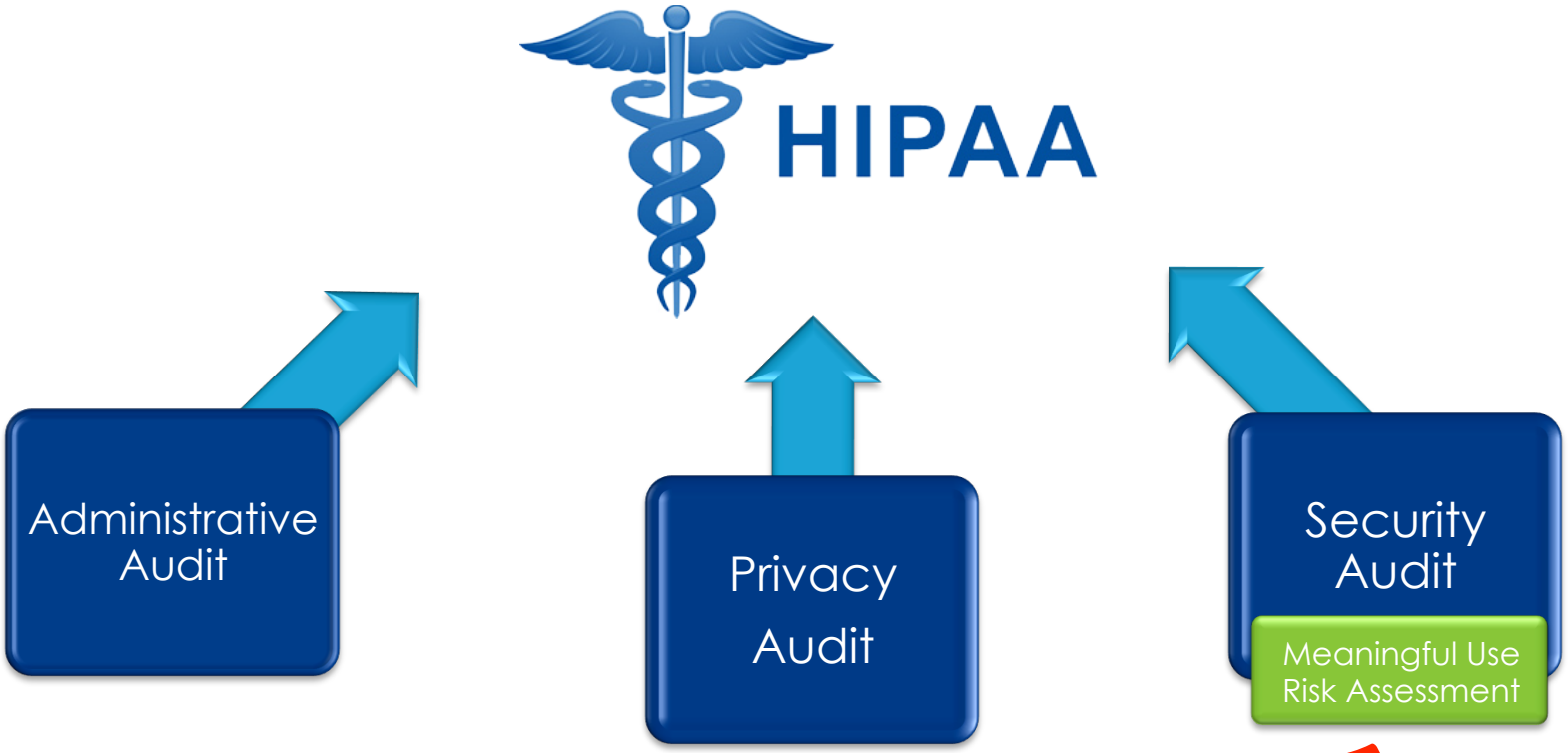
CEs fail to understand the difference between HIPPA and HITECH.

- *"Problems were discovered with most or all CE's policies and procedures including those for performing Risk Assessments"*[1]
- *"89% of the entities audited were non-compliant in one or more areas. Security Rule issues accounted for 60% of the findings and observations, while the Privacy and Breach Notification Rules yielded 30% and 10% respectively"*[2]

Compliancy Group
Achieve.Illustrate.Maintain.
Compliance Simplified

[1]: CMS Compliance Reviews, "HIPAA Compliance Review Analysis and Summary of Results"
[2]: http://www.healthcare-informatics.com/article/ocr-audits-forewarned-forearmed

A Risk Assessment is NOT enough!



Completing a risk assessment does not make you HIPAA compliant.

Compliancy Group
Achieve.Illustrate.Maintain.
Compliance Simplified

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

Compliancy Group
Achieve.Illustrate.Maintain.
Compliance Simplified

The HIPAA Compliance Puzzle

Compliancy Group
Achieve.Illustrate.Maintain.
Compliance Simplified

Compliance Plan

Step 1. Assess where you are against the regulation (GAP)

- The key to a risk analysis is auditing yourself against the administrative, technical, and physical aspects of HIPAA
- A risk analysis will help you attest to Meaningful Use Stage 1 Core Requirement 15

Step 2. Remediation Plan

- Prove that you remediated the deficiencies identified in the risk analysis
- Policies & Procedures, Training, and Attestation

Compliance Plan (Continued)

Step 3. How do you prove it? Successful compliance plans address:

- **Administration and Technical**
  - Policies and Procedures
- **IT security**
  - Devices installed and maintained within your organization
- **Physical**
  - Security within physical locations of your practice(s)

(MU Stage 2 Core Requirement 9 requires remediation of found deficiencies during the risk analysis to be documented and completed)

Step 4. Maintain your compliance

- As the regulations, staff, and practice changes

Questions?

For more information, contact:

Sales & Demo Scheduling Questions

Marc Haskelson

855.854.4722 ext 507

marc@compliancygroup.com

HIPAA Questions

Bob Grant

855.854.4722 ext 502

bob@compliancygroup.com

Compliancy Group
Achieve.Illustrate.Maintain.
Compliance Simplified

The Total Compliance Solution

The Guard

Compliance
Simplified

Achieve
Compliance Coaching

Illustrate
Seal of Compliance

Maintain
HIPAA Hotline

HIPAA Compliant

- All aspects of compliance satisfied
- Compliance *simplified*!
- Compliance Coach walks the client through the whole journey
- No client has ever failed an audit!

Find out more now:

www.compliancy-group.com
855.85 HIPAA (855.854.4722)

Thank You For Attending

Compliancy Group
Achieve.Illustrate.Maintain.
Compliance Simplified