Compliancy Group
Achieve.Illustrate.Maintain.
Compliance Simplified

HIPAA 101: The 30-Minute Guide to Understanding Compliance

Compliancy Group
Achieve.Illustrate.Maintain.
Compliance Simplified

HIPAA Webinar Series:

- **HIPAA 101: The 30-Minute Guide to Understanding Compliance**
  - Today

Compliancy Group Free Education Series

- Upcoming & past webinars:
  http://compliancy-group.com/webinar/

Free Resources (whitepapers, articles, infographics)
https://compliancy-group.com/blog/

Please ask questions If we are unable to address them during the webinar, you will receive a response via email within 24-48 hours.

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

Are YOU HIPAA Compliant?

We are HIPAA compliant…

Risk Assessments

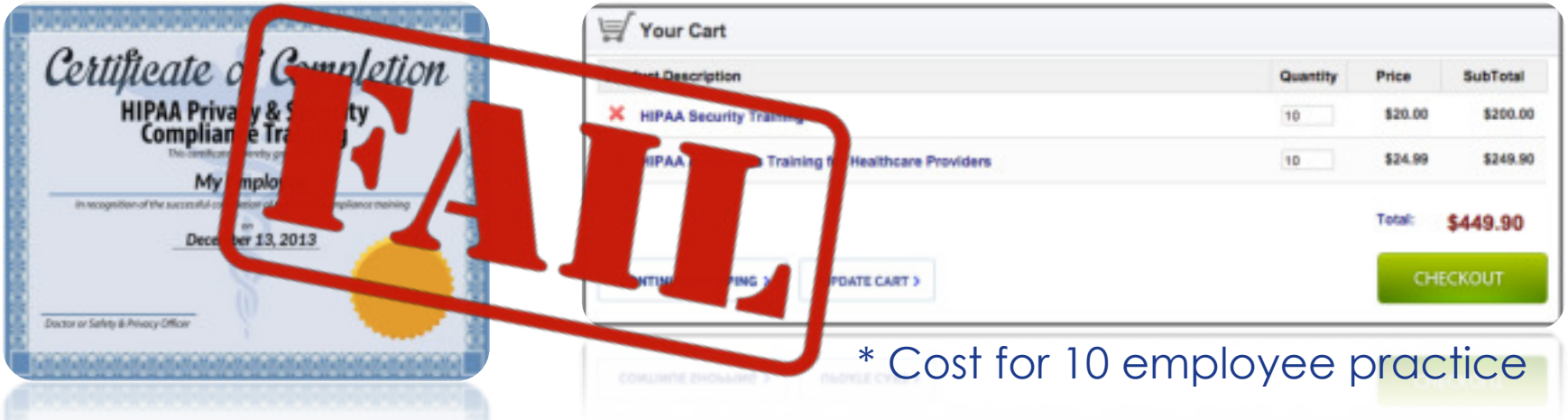
- I had an expensive Security Risk Assessment done
- Am I HIPAA compliant?

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

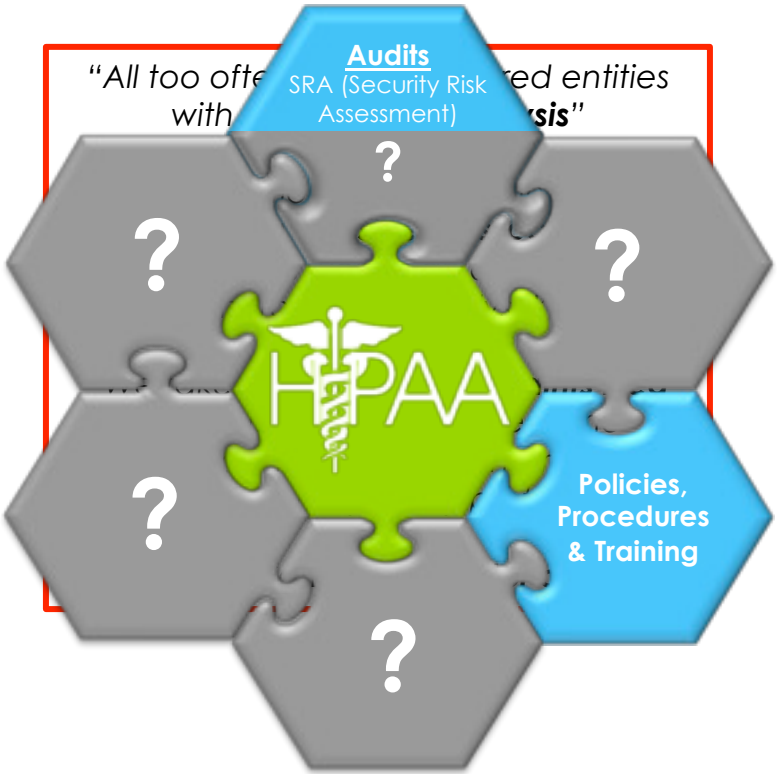
Avoidable Breach

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

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:
    - **$6.2 Million** in 2015
    - **$24 Million** in 2016
    - **$17.1 Million** so far in 2017*
  - Three prison sentences
  - Medical license revoked
  - State Attorney General levying fines



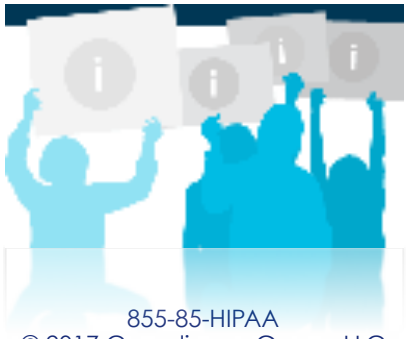
http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html

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



Important Definitions (Continued)

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

What Information Does HIPAA Protect?

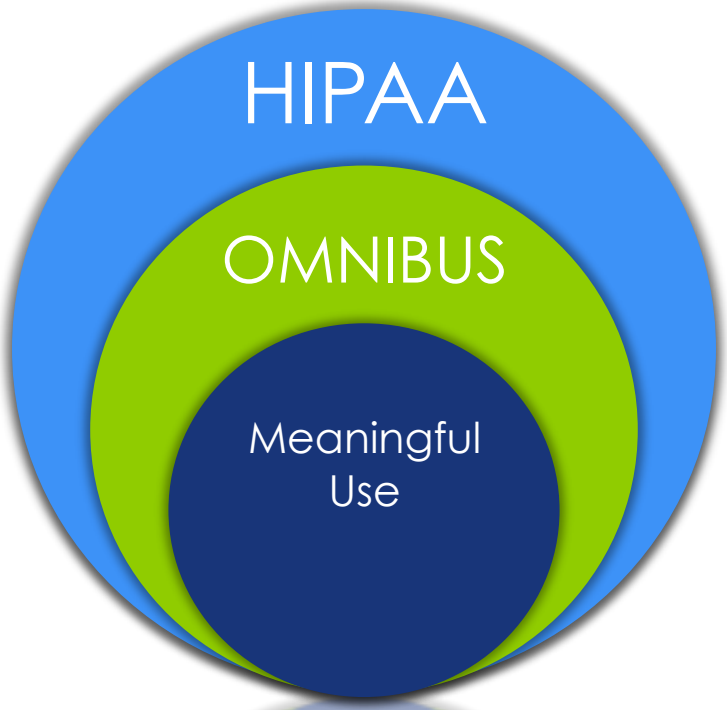
PHI may include any of the following:

- 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

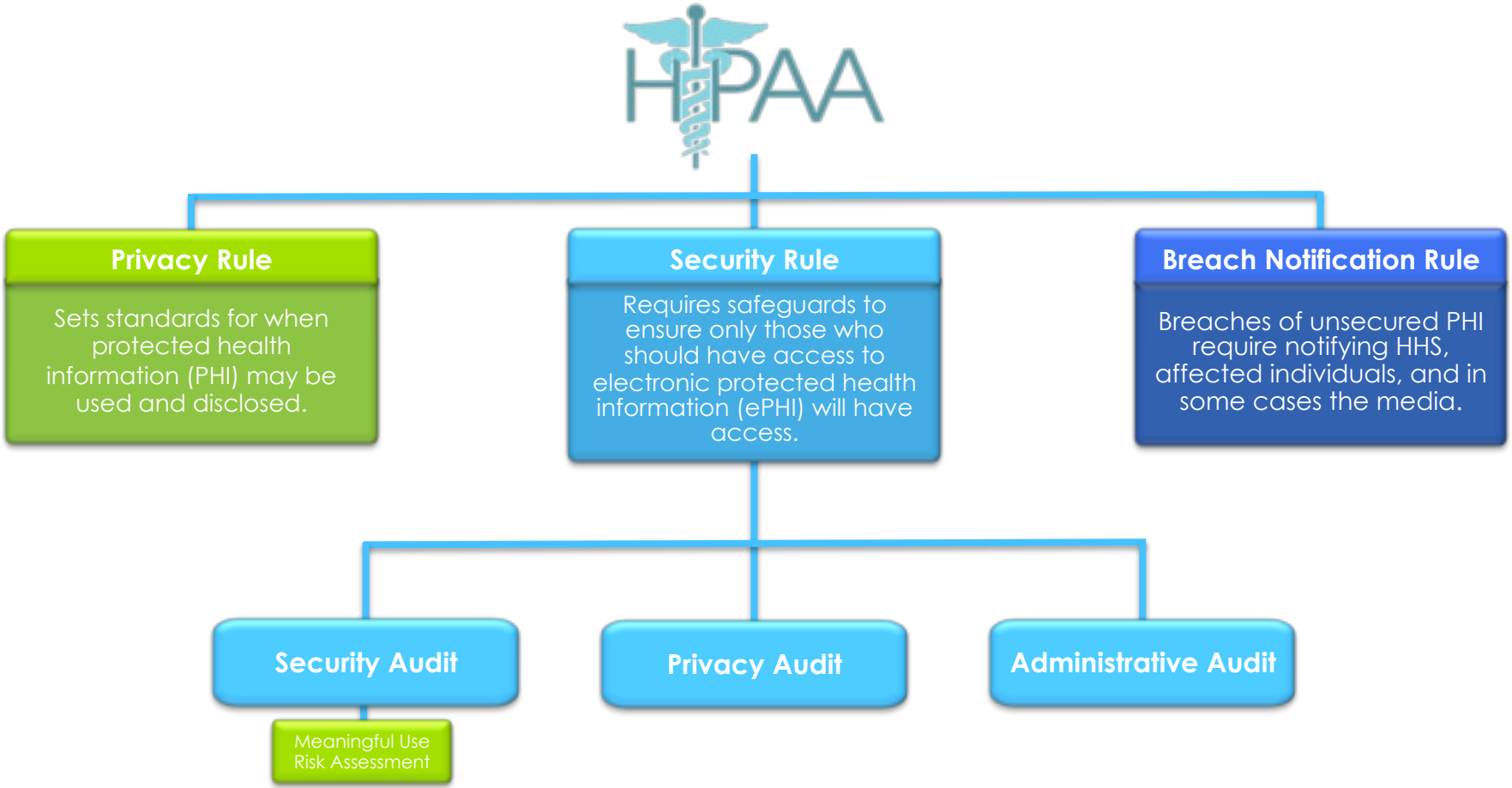
- **Compliance vs. Security**
  - Fines vs. Risk
- **HIPAA/HITECH**
  - Protect patient confidentiality while furthering innovation and patient care
  - Privacy Rule and Security Rule
- **Omnibus**
  - Business Associates must be HIPAA compliant
  - Covered Entities must have BAAs
    - Conduct Due Diligence
  - 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
- Prevention
  - System Hardening
  - Penetration Testing
  - Vulnerability Scan
- Detection
  - Behavioral monitoring
  - Network Security Monitoring

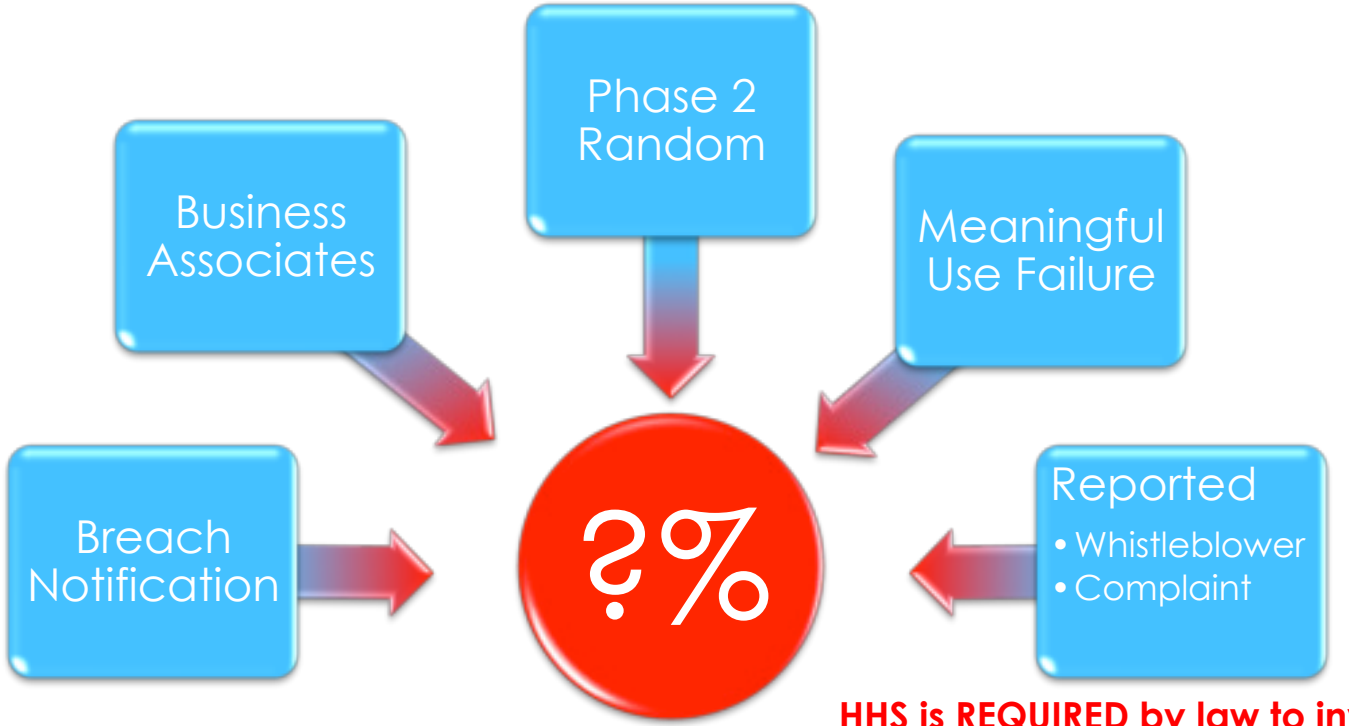


Omnibus Rule

- 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 a Technical **Due Diligence**
- Contracting with subcontractors
  - BA liability flows to all subcontractors

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

Causes Of A HIPAA Audit



HHS is REQUIRED by law to investigate ALL HIPAA violation complaints

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**

"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

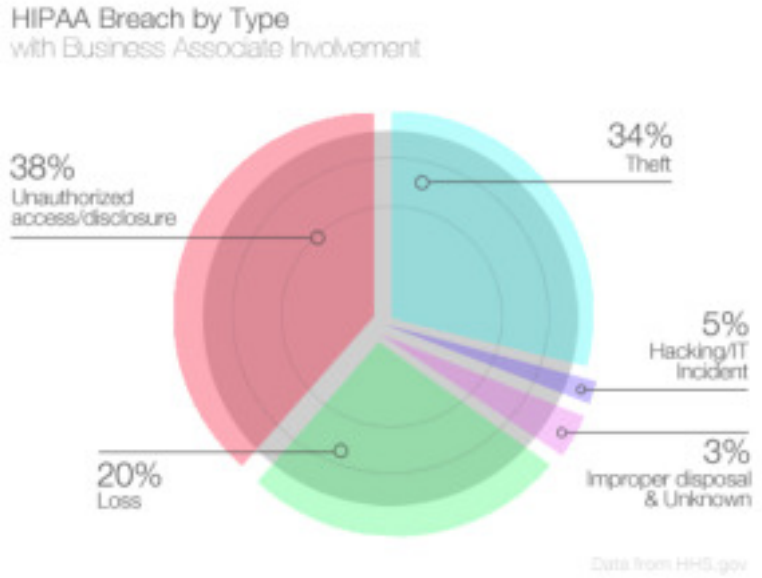
$31,000 Mistake

- 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**

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

PHI Breaches

- Caused by Theft or Loss-related reasons

- Involved Business Associates

- Caused by Hacking or IT incident

https://www.healthcare-informatics.com/news-item/cybersecurity/study-30-percent-patient-data-breaches-involve-business-associates

HHS Breach Portal AKA "**Wall of Shame**"

What is a meaningful breach?

	Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
	Aetna Inc.	CT	Health Plan	5002	06/20/2017	Unauthorized Access/Disclosure	Other
	Little River Healthcare	TX	Healthcare Provider	542	06/16/2017	Theft	Laptop
	Airway Oxygen, Inc.	MI	Healthcare Provider	500000	06/16/2017	Hacking/IT Incident	Network Server
	Texas Health and Human Services	TX	Health Plan	1842	06/15/2017	Improper Disposal	Paper/Films
	SSM DePaul Medical Group (Dr. Syed Khader)	MO	Healthcare Provider	838	06/09/2017	Theft	Other
	Tennessee Rural Health Improvement Association	TN	Health Plan	588	06/08/2017	Loss	Paper/Films
	Southwest Community Health Center	CT	Healthcare Provider	6000	06/07/2017	Theft	Desktop Computer, Laptop
	Toth Enterprises II d/b/a Victory Medical	TX	Healthcare Provider	2000	06/05/2017	Unauthorized Access/Disclosure	Email, Paper/Films
	North Dakota Department of Human Services	ND	Health Plan	2452	06/01/2017	Improper Disposal	Paper/Films
	LKM ENTERPRISES, INC.	OK	Healthcare Provider	3400	06/01/2017	Theft	Desktop Computer, Laptop
	CCHI Insurance Services	CA	Health Plan	1000	06/01/2017	Theft	Desktop Computer, Electronic Medical Record, Email, Network Server
	Advanced ENT Head & Neck Surgery	CA	Healthcare Provider	15000	05/31/2017	Theft	Desktop Computer, Electronic Medical Record, Email, Laptop, Other, Other Portable Electronic Device, Paper/Films
	N. Fred Eaglstein, D.O. d/b/a Dermatology and Laser Center	FL	Healthcare Provider	2000	05/30/2017	Unauthorized Access/Disclosure	Electronic Medical Record
	Arizona Department of Health Services	AZ	Healthcare Provider	2500	05/26/2017	Loss	Paper/Films
	Sound Community Services, Inc.	CT	Healthcare Provider	1278	05/26/2017	Hacking/IT Incident	Email
	Beacon Health System	IN	Healthcare Provider	1239	05/26/2017	Unauthorized Access/Disclosure	Electronic Medical Record

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**

"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

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

The HIPAA Compliance Puzzle

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

Marc Haskelson
President & CEO
855-854-4722 Ext 502
Marc@compliancygroup.com

Compliancy Group
855-85-HIPAA | 855-854-4722
info@compliancygroup.com
www.CompliancyGroup.com