EXCLUSIVELY FOR

The Arc New York

Cerebral Palsy Associations of New York State

Real people. Realizing potential.

HIPAA UPDATE & SUCCESS STRATEGIES

SEMEL CONSULTING

So What?

Why is this important?

Mike Damiano
Executive Director

The Arc®
Allegany-Steuben
New York

SEMEL CONSULTING

Agenda

- **KEYNOTE – Why is this important?**
  - Mike Damiano, Executive Director, The Arc of Allegany – Steuben
- **HIPAA Update**
  - Horror Stories, Recent Penalties, & Lessons Learned
  - Proposed HIPAA Changes
- **STRATEGIES TO PREVENT LONG-TERM PROBLEMS**
- **TOPICS YOU ASKED FOR**
- **Q&A**

3 BUSINESS REASONS
YOU WANT TO PAY ATTENTION

1

PROTECT YOUR REPUTATION

2

SAVE MILLIONS OF DOLLARS

3

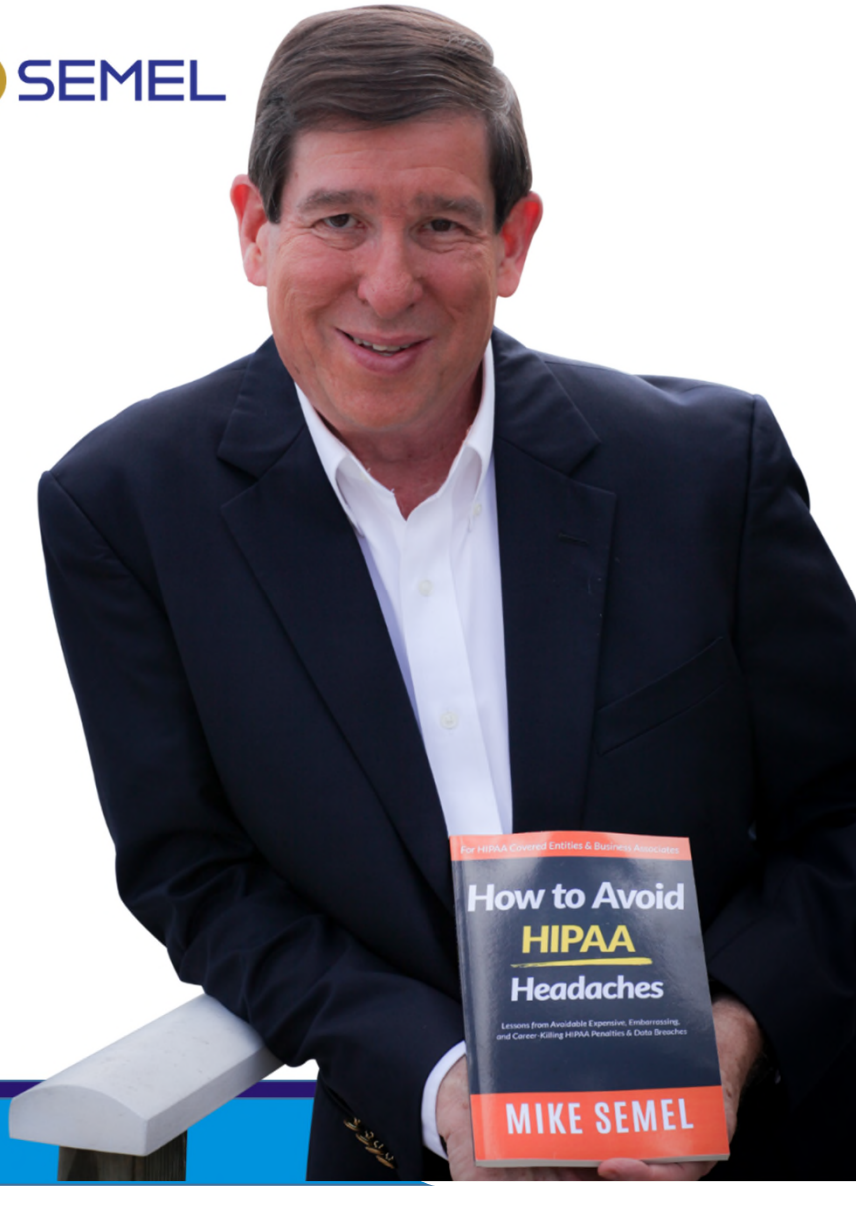
SAVE YOUR CAREER

SEMEL CONSULTING

Why I Care

MIKE SEMEL

- EMT & Fire Dept. Rescue Captain
- IndyCar Safety Team – 19 years
- IT Support Business Owner
- Hospital Chief Information Officer (CIO)
- K-12 School District CIO
- Certified in Cybersecurity & Compliance

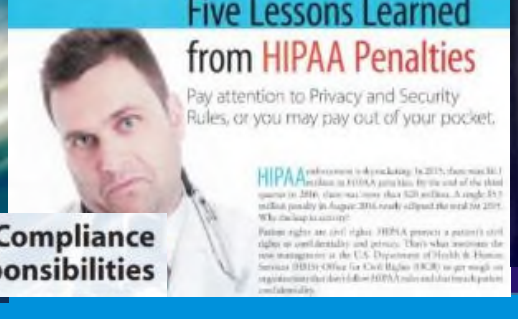


CMMC – Cybersecurity Maturity Model Certification

New Requirements for Defense Contractors

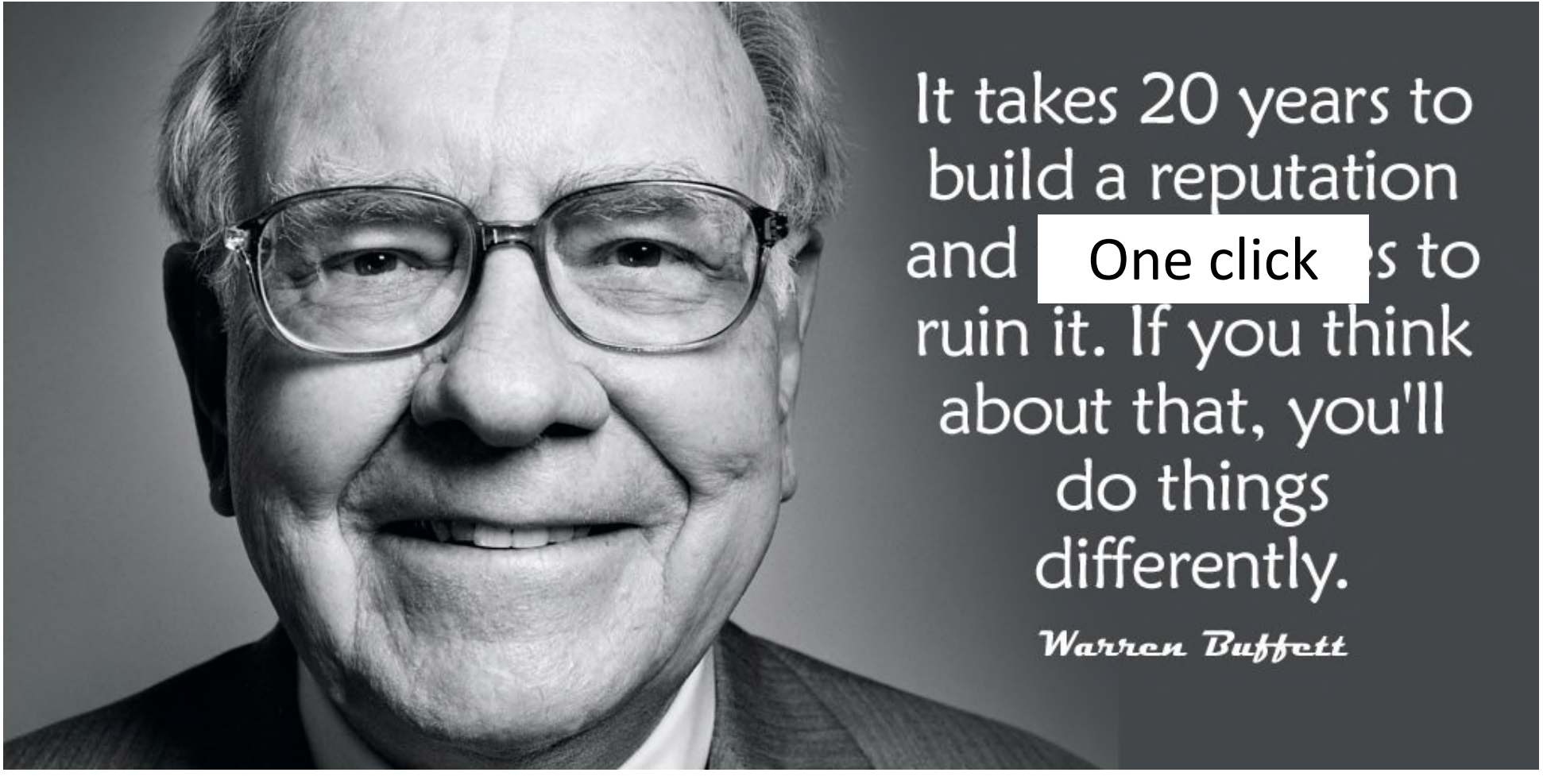
Interim Rule until CMMC is rolled out over 5 years

Speaking, Writing



SEMEL CONSULTING


Cerebral Palsy Associations
of New York State
cpofnys.org



SEMEL CONSULTING

Cyber Security
Is a BUSINESS problem
With a TECHNICAL solution

Compliance is Anything Someone Else Makes You Do

Compliance Requirements

- Federal & State Laws
- Industry Regulations
- Contracts
- Insurance Policies

A HIPAA HORROR STORY

SEMEL CONSULTING

Patient Data Published to Internet

- Cottage Health's IT company installed a server and accidently published it to the Internet
- Patients Googled Themselves & Got their Medical Records, then sued
- Vendor did not have insurance so Cottage Health filed a claim with its cyber-liability carrier, Columbia Casualty
- Lawsuit settled for $ 4.1 million
- Columbia Casualty paid settlement and lawyer's fees, but said it was still investigating…

Will Your Cyber Liability Insurance Pay Off?

Insurer Seeks Breach Settlement Repayment

Alleges Client Failed to Follow 'Minimum Practices'

Columbia Casualty alleges that Cottage Health's application for coverage under the Columbia policy "contained misrepresentations and/or omissions of material fact that were made negligently or with intent to deceive concerning Cottage's data breach risk controls," according to the insurer's lawsuit.

Plus State & Federal Penalties

HHS.gov
Health Information Privacy

Cottage Health Settles Potential Violations of HIPAA Rules for $3 Million

XAVIER BECERRA
Attorney General

Attorney General Becerra Announces $2 Million Settlement Involving Santa Barbara-based Cottage Health System Over Failure to Protect Patient Medical Records

$ 9,100,000

- Failed to conduct an accurate and thorough assessment of the potential risks
- Failed to implement security measures sufficient to reduce risks
- Failed to perform periodic technical and non-technical evaluations
- Failed to obtain a written business associate agreement with a contractor that maintained ePHI on its behalf.

SEMEL CONSULTING

EXCLUSIVELY FOR

The Arc New York

Cerebral Palsy Associations of New York State

Real people. Realizing potential.

HIPAA UPDATE

SEMEL CONSULTING

Right of Access Initiative

"OCR created the Right of Access Initiative to address the many instances where patients have not been given timely access to their medical records.

Health care providers, large and small, must ensure that individuals get timely access to their health records, and for a reasonable cost-based fee," said OCR Director Roger Severino.

20

Right of Access Initiative

Patients are supposed to receive their records in 30 days, with one 30-day delay for a good reason.

Patients should be charged only actual costs to provide their records, with a Safe Harbor of $6.50 to avoid a complaint investigation.

21

13 Right to Access Enforcements since September 2019

EXAMPLE:

NON-PROFIT - Housing Works Inc. – provides healthcare, homeless services, advocacy, job training, reentry services, and legal aid to people living with and affected by AIDS.

INCIDENT: **July 2019 – complaint that in June 2019 HW failed to provide a patient with a copy of his medical records.** The OCR provided HW with technical assistance & closed the case. In August 2019 a second complaint was received. OCR opened an investigation and in November 2019 the patient received his records.

PENALTY - $ 38,000

HIPAA Penalties

2014 + 2015

$ 14 million

2016 + 2017

$ 42 million

2018 + 2019

$ 41 million

2020

$ 13.5 million

$ 3,000,000 HIPAA Penalty

- **Medical Imaging Practice**
  - Exposed 300,000 patient records to the Internet
  - Failed to conduct an “accurate and thorough” risk analysis
  - Failed to implement adequate security measures
  - **Failed to sign Business Associate Agreements with its vendors, including its IT support vendor and third-party data center**

$ 100,000 HIPAA Penalty

- **March 2020 – 1-Doctor Practice - $ 100,000**
  - Filed a breach report related to a dispute with a Business Associate
  - Failed to conduct an “accurate and thorough” risk analysis
  - Failed to implement adequate security measures

$ 1,040,000 Non-Profit HIPAA Penalty

- **July 2020 – Non-Profit**
  - Lost an unencrypted laptop
  - **Failed to encrypt all devices used for work purposes**
  - Failed to track or inventory all devices that access the network or contain ePHI
  - Did not have Business Associate Agreements in place

Other HIPAA Enforcements – 2020

- **September 21 – Orthopedic Clinic - $ 1.5 million**
- **September 23 – Business Associate - $ 2.3 million**
- **September 25 – Health Plan - $ 6.85 million**
  - **Failed to conduct an “accurate and thorough” risk analysis**
  - **Failed to implement adequate security measures**

Don’t Assume Everything is OK

We have helped many non-profits by creating their first-ever accurate & thorough security risk analysis.

Don’t Assume Everything is OK

We have advised many non-profits to implement - for the first time - adequate security measures that will stand up to an audit.

Don’t Assume Everything is OK

We have many non-profits properly manage their Business Associate relationships.

Don’t Assume Everything is OK

We have helped many non-profits comply – for the first time – with the requirements of their cyber liability insurance policy.

EXCLUSIVELY FOR

The Arc New York

Cerebral Palsy Associations of New York State

Real people. Realizing potential.

PROPOSED HIPAA CHANGES

SEMEL CONSULTING

Federal Rulemaking Process

1. House and Senate pass law
2. President signs law
3. Agency responsible writes rule
4. Agency publishes Notice of Proposed Rulemaking (NPRM) in Federal Register & asks for comments
5. After comment period agency releases final rule in Federal Register
6. Agency begins enforcement 6 months later

33

HIPAA Omnibus Rule

HITECH Act – February 17, 2009

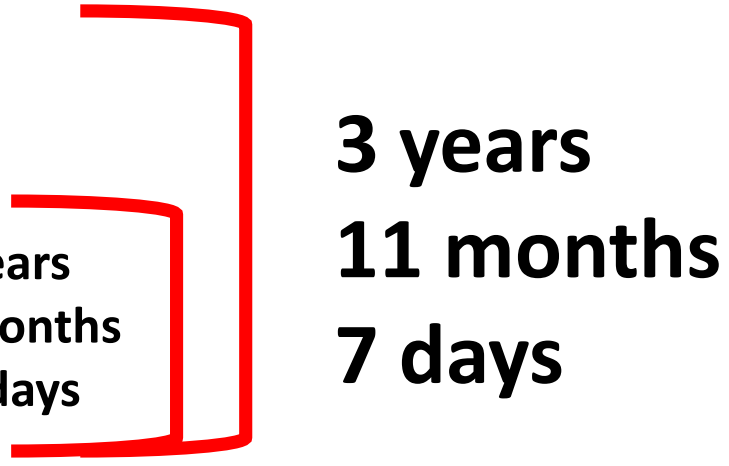
NPRM – July 14, 2010

HIPAA Omnibus Final Rule

Announced January 24, 2013

Effective March 26, 2013

Enforced September 23, 2013



HIPAA Privacy Rule NPRM

- Announced December 10, 2020
- Designed to “Empower Patients, Improve Coordinated Care, and Reduce Regulatory Burdens”
- 357 pages
- Comment period ends February 8, 2021

HIPAA Privacy Rule NPRM – Empowering Individuals

- Letting patients review and capture images of their medical records
- Shortening response time to 15 days to provide records, with a delay of no more than 15 more days
- Reducing identity requirements
- Amending the current fee structure
- Requiring the posting of estimated fee schedules

HIPAA Privacy Rule NPRM - What affects you

Clarifying the scope of covered entities' abilities to disclose PHI to social services agencies, community-based organizations, home and community-based service (HCBS) providers, and other similar third parties that provide health-related services, to facilitate coordination of care and case management for individuals.

HIPAA Privacy Rule NPRM – Best Interests of Individuals

- Allowing the disclosure of PHI needed to improve care for health emergencies
- Modifying “professional judgment” to “good faith” belief disclosure is in best interests
- Changes “serious and imminent threat” to “serious and reasonably foreseeable”
- Disclosures to family members and other caregivers unless individual objects

HIPAA Privacy Rule NPRM – Care Coordination

- Disclosures exempt from minimum necessary standard for Treatment
- Does not include disclosures for Operations
- Should streamline requests for PHI for Treatment

HIPAA Privacy Rule NPRM – Notice of Privacy Practices

- Eliminate requirement for written acknowledgement of NPP & retention for 6 years
- Modify content of NPP with new changes

HIPAA Privacy Rule NPRM – TRS

- Increases approved disclosures to Telecommunications Relay Services (TRS) for the deaf, hard of hearing, deaf-blind, or speech disability
- Without obtaining an individual's authorization

HIPAA Security Rule Changes – HR 7898

One Hundred Sixteenth Congress
of the
United States of America

AT THE SECOND SESSION

Begun and held at the City of Washington on Friday, the third day of January, two thousand and twenty

An Act

To amend the Health Information Technology for Economic and Clinical Health Act to require the Secretary of Health and Human Services to consider certain recognized security practices of covered entities and business associates when making certain determinations, and for other purposes.

HIPAA Security Rule Changes – House of Rep. HR 7898

- Introduced in HR – July 31, 2020
- Passed by HR – December 9, 2020
- Passed by Senate – December 19, 2020
- Signed by President – January 5, 2021

- Will go through Rulemaking (NPRM) Process

HIPAA Security Rule Changes – House of Rep. HR 7898

- SAFE HARBOR LAW
- Mitigate fines
- Terminate audits early and favorably, if:
- Covered Entity or Business Associate demonstrates it has, for the previous 12 months, implemented recognized security practices

HIPAA Security Rule Changes – House of Rep. HR 7898

- SAFE HARBOR LAW
- Refers to the National Institute of Standards & Technology (NIST)
- Should end up with a rule recommending the implementation of the NIST Cybersecurity Framework (CSF) 98 cybersecurity controls

Comply With

By Implementing

LAWS

HIPAA
HITECH
NY SHIELD ACT

RULES

HIPAA SECURITY RULE
PCI – DSS – CREDIT CARDS
DFARS

FRAMEWORKS

NIST CSF
NIST 800-53
NIST 800-171
ITIL
ISO 27001
CMMC

The NIST Cybersecurity Framework (CSF)

5 Functions

23 Categories

98 Subcategories

Achievable

Affordable

Aligns with regulations

SEMEL CONSULTING

The Swiss Army Knife of Cybersecurity & Compliance

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

CSF

HIPAA

PCI-DSS

STATE LAWS

CYBER INSURANCE

SEMEL CONSULTING

EXCLUSIVELY FOR

The Arc New York

Cerebral Palsy Associations of New York State

Real people. Realizing potential.

YOUR REQUESTS

SEMEL CONSULTING

CYBERSECURITY IN THE PANDEMIC

- Work at Home creates many cybersecurity challenges
- Some HIPAA telehealth restrictions were lifted to allow doctors to provide remote care
- Hackers are taking advantage of everyone's stress levels by increasing phishing attacks and scams
- All the rules still apply

HIPAA BREACH ASSESSMENT – Are we asking the right questions?

- Breach exceptions are narrow, not a wide loophole to exploit
- Data breaches require forensic examinations by certified specialists
- Lost unencrypted devices are assumed to have been breached
  - **Can you PROVE a lost device was encrypted?**
- All breaches of PHI must be reported
- Ransomware is a reportable breach because the data was accessed without authorization

SEMEL CONSULTING

ACCOUNTING OF DISCLOSURES

- **What are the requirements of a covered entity?**
  - **Provide individual with a list of disclosures of their PHI, including:**
    - **Date**
    - **To Whom, including address**
    - **Description of information**
    - **Purpose of Disclosure**
    - **Within 60 days**

ACCOUNTING OF DISCLOSURES

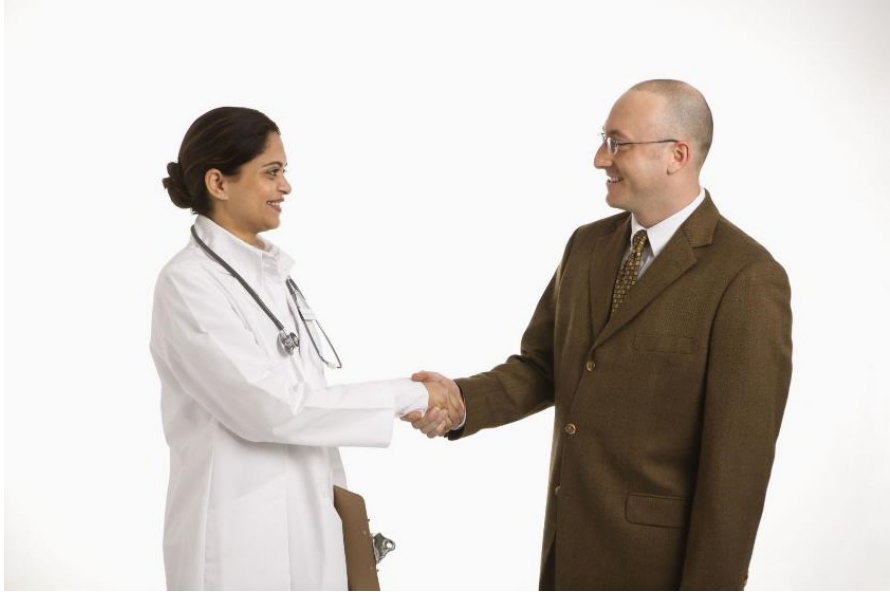
- **Research (if not de-identified)**
- **Marketing Activities**
- **Court Orders, subpoenas, state reporting**
- **Public Health Activities**
- **Investigations, Medicare Fraud Audit**
- **Decedents**
- **Organ Donation**
- **Worker's Comp**
- **Mistakes**

ACCOUNTING OF DISCLOSURES

- **EXCEPT FOR…**
  - **Treatment, Payment, and Health Care Operations (TPO)**
  - **To the individual**
  - **Directory Information**
  - **Correctional Institutions & Law Enforcement**

BUSINESS ASSOCIATE OVERSIGHT & LIABILITY

- **What is Your Responsibility?**
  - Select Responsible Vendors
  - Reasonably Validate Compliance
  - Sign BA Agreements
- **What is Your Liability?**
  - **You can be held responsible for what a BA does.**



COVID TESTING OF EMPLOYEES

- ADA, not HIPAA, covers employee medical records, even if the information is not about a disability
- Medical information includes diagnosis, treatment, and requests for special accommodations
- Medical information must be stored separately from an employee's personnel file
- Don't share the name, even though others may figure it out

EXCLUSIVELY FOR

The Arc New York

Cerebral Palsy Associations of New York State

Real people. Realizing potential.

STEPS TO SUCCESS

SEMEL CONSULTING

Strategies, then tactics

Compliance First

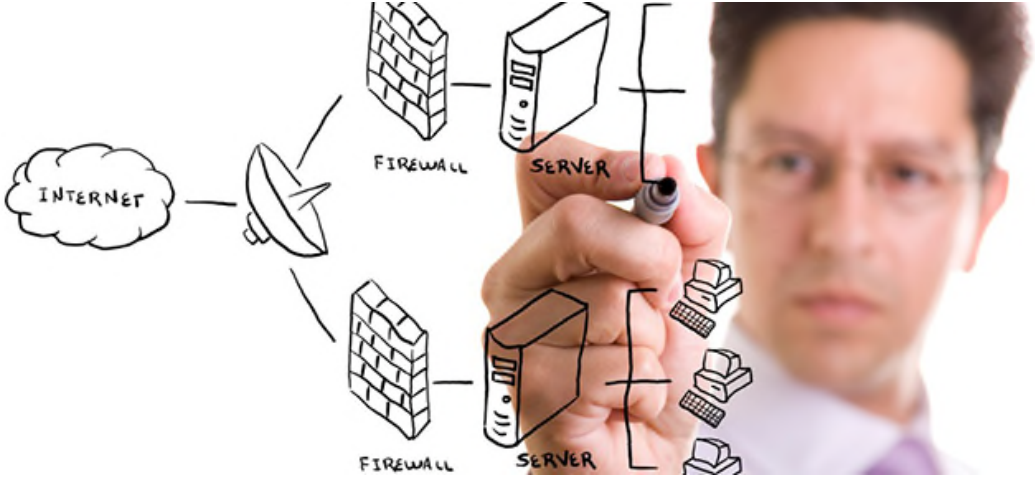
then select from remaining options

Non-Compliant Solution

Compliant Solution

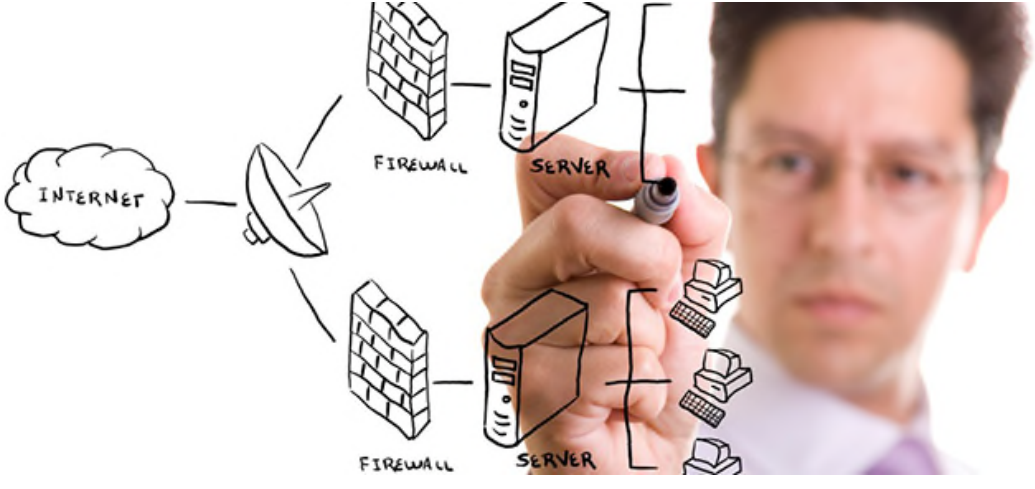
FIREWALL EXAMPLE

- HIPAA requires a network firewall with Active Intrusion Prevention
- Well-meaning IT Director wanted to save his organization's money
- Purchased a router to connect the network to the Internet
- Wrote some programming code to identify attempted intrusions



FIREWALL EXAMPLE

- Did not include all the features that come in a commercial firewall
- Was not implemented by a certified firewall security specialist
- Would not have stood up to the HIPAA requirements if there had been a breach
- And…



Cyber Insurance Policy Application

I. Information Security & Privacy Controls		
1. Does the Applicant have and require employees to follow written computer and information systems policies and procedures?	☑ Yes	☐ No
2. Does the Applicant use the following controls:		
A. Commercially available Firewall protection:	☑ Yes	☐ No
B. Commercially available Anti-Virus protection:	☑ Yes	☐ No

Protect all data

including voice messages

Voice Over Internet Protocol (VOIP) PHONE SYSTEM

- VOIP phone systems may be local or in the Cloud
- Voice Messages with PHI are saved as data
- May be forwarded to email or accessed through a portal
- HIPAA requires encryption of PHI in-transit and at-rest (stored)
- Most VOIP systems do not encrypt voice messages

Voice Over Internet Protocol (VOIP) PHONE SYSTEM

- Both the local vendor that supports the system, and the manufacturer that connect in to support the system, must comply with HIPAA as Business Associates
- Full implementation of the Security Rule
- Business Associate Agreements

No Seals

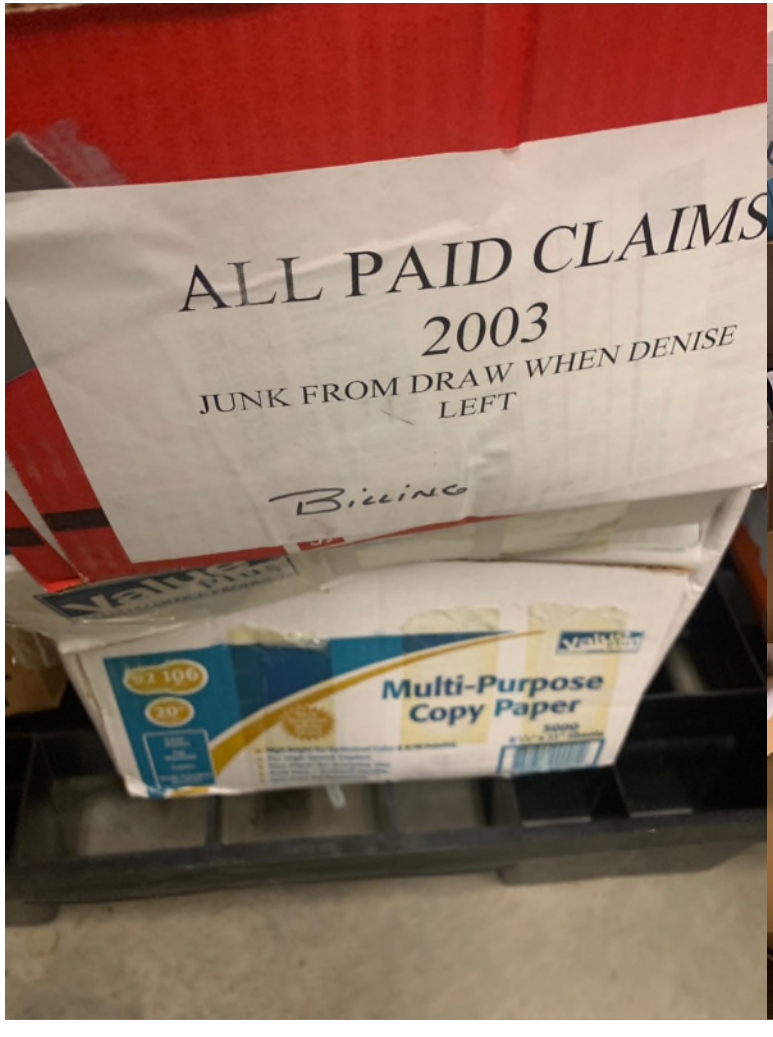
FTC Consumer Fraud Penalty

- Federal Trade Commission Deceptive Marketing & Unfair Information Security Practices
- December 16, 2020
- SkyMed breached membership info for 130,000 individuals
- "SkyMed deceived consumers by displaying for nearly five years a "HIPAA Compliance" seal on every page of its website"

69

Stop Ignoring Paper

It won't go away by itself.



71

Hope is not a business strategy

Contact us with questions.

mike@semelconsulting.com

rose@semelconsulting.com

FREE CYBERSECURITY & COMPLIANCE CHECKUP

https://semelhipaa.com/checkup

SEMEL CONSULTING