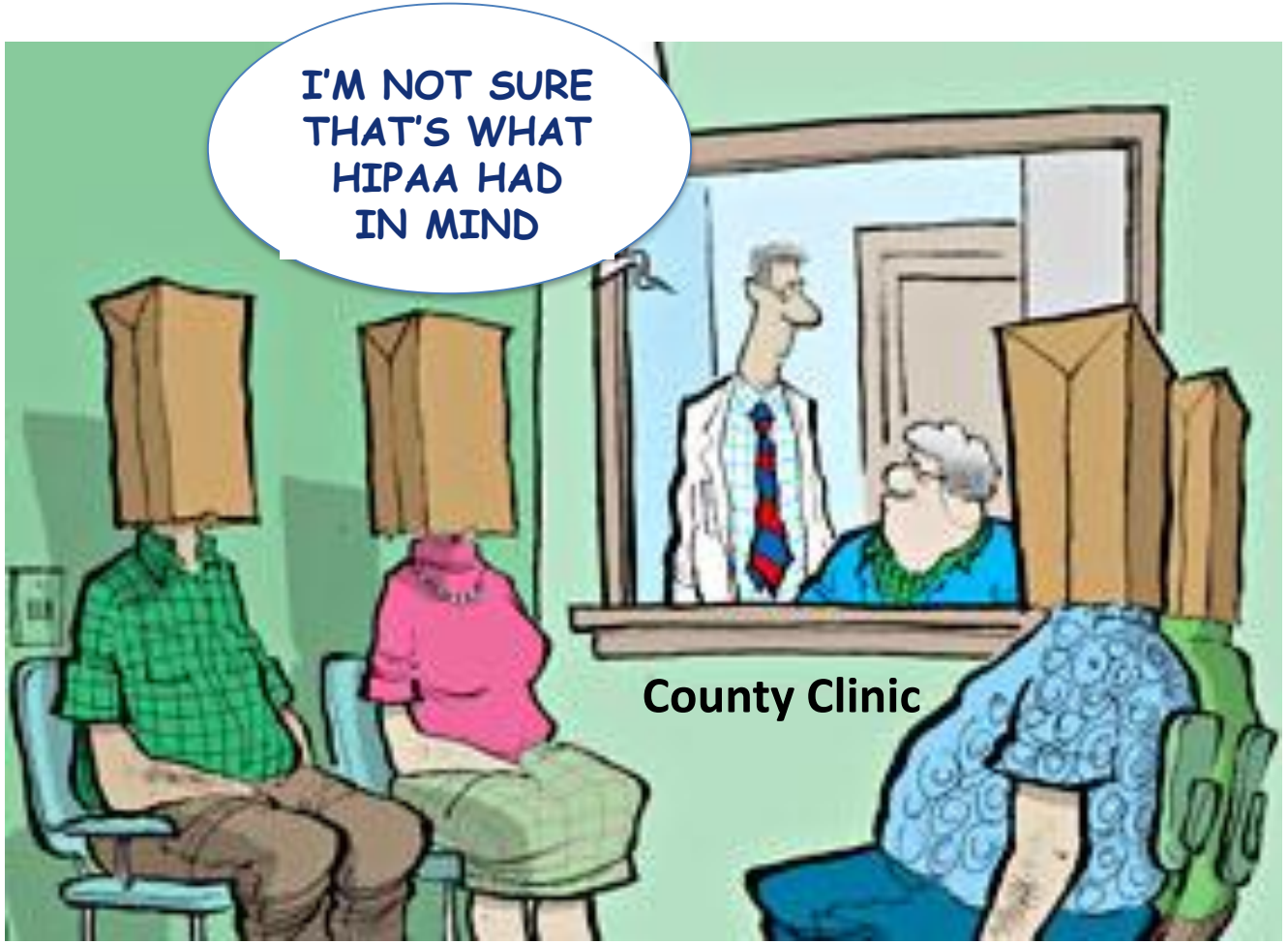
Why Security & Compliance are Executive Responsibilities

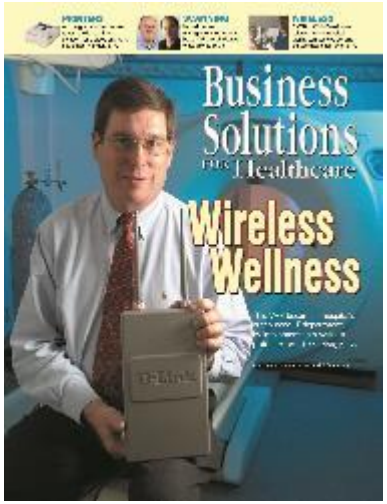


© Copyright 2016 Semel Consulting LLC ALL RIGHTS RESERVED – Slides and Cartoons may not be shared without permission

SEMEL CONSULTING

Mike Semel

- 35-year IT business owner/manager
- 12 year certified HIPAA Professional
- Hospital CIO (2004 – 2006)
- School District CIO (2007 – 2012)
- Certified HIPAA Administrator
- Certified HIPAA Security Professional author
- Certified Security Compliance Specialist
- Certified Health IT Consultant
- Certified Business Continuity Professional
- Chair, CompTIA Security Community (retired)
- CompTIA Security Trustmark (holder, development team, author- quick reference guide, coach)



Mike Semel
President
Chief Compliance Officer
SEMEL Consulting

© Copyright 2016 Semel Consulting LLC ALL RIGHTS RESERVED – Slides and Cartoons may not be shared without permission

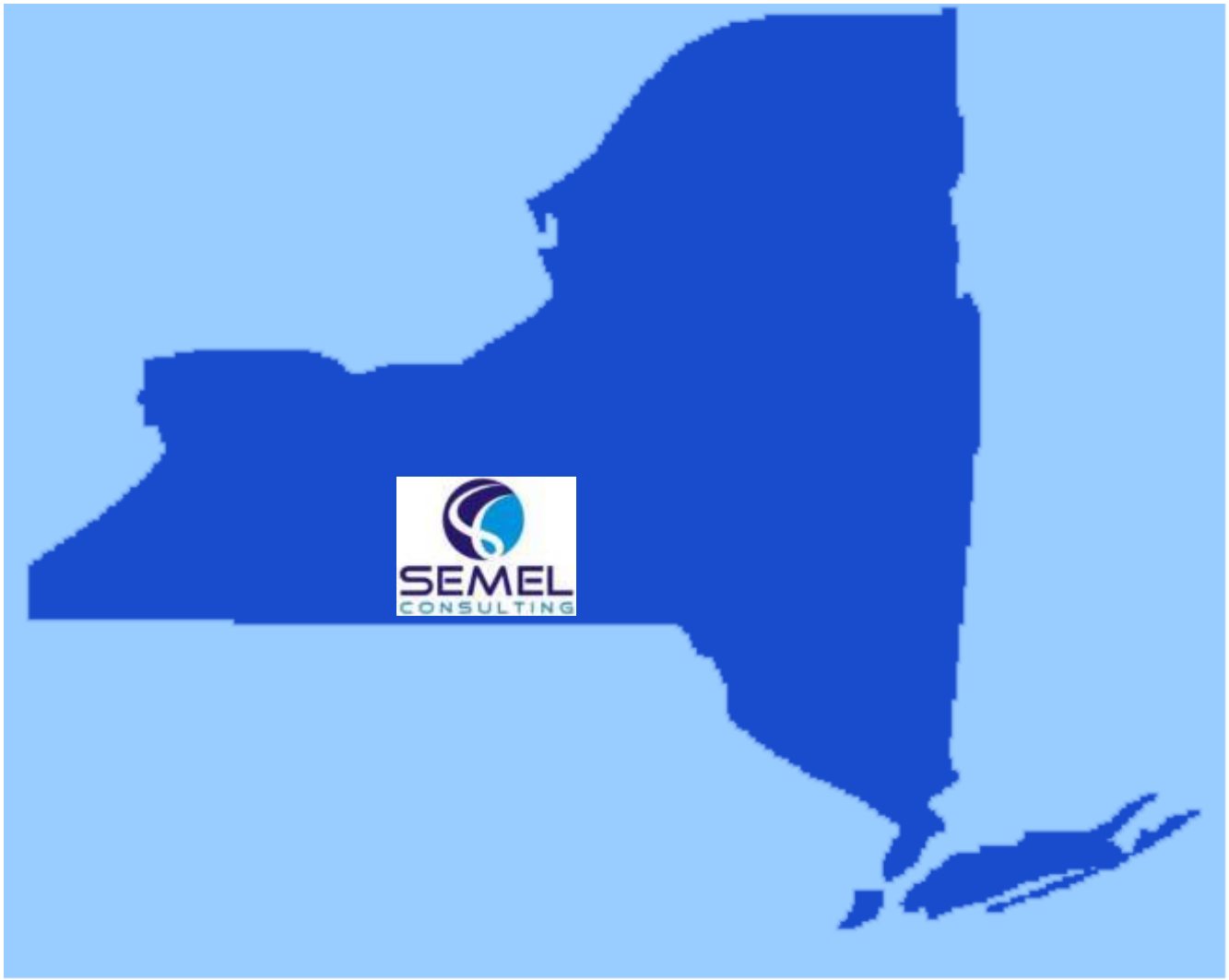
New Title

- Grandpa

© Copyright 2016 Semel Consulting LLC ALL RIGHTS RESERVED – Slides and Cartoons may not be shared without permission

SEMEL CONSULTING

New York Office



© Copyright 2016 Semel Consulting LLC ALL RIGHTS RESERVED – Slides and Cartoons may not be shared without permission

SEMEL
CONSULTING

Things Have Changed

Then & Now

© Copyright 2016 Semel Consulting LLC ALL RIGHTS RESERVED – Slides and Cartoons may not be shared without permission

SEMEL CONSULTING

Airport

- Then - Convenience

- Now- Security

© Copyright 2016 Semel Consulting LLC ALL RIGHTS RESERVED – Slides and Cartoons may not be shared without permission

SEMEL CONSULTING

Health Care

- Then - Convenience

- Now- Safety

© Copyright 2016 Semel Consulting LLC ALL RIGHTS RESERVED – Slides and Cartoons may not be shared without permission

SEMEL CONSULTING

Medical Records

- Then - Paper

- Now- Electronic

© Copyright 2016 Semel Consulting LLC ALL RIGHTS RESERVED – Slides and Cartoons may not be shared without permission

SEMEL CONSULTING

Stealing 10,000 medical records

- Then

- Now

© Copyright 2016 Semel Consulting LLC ALL RIGHTS RESERVED – Slides and Cartoons may not be shared without permission

SEMEL CONSULTING

IT Company, IT Department

- **Then –**

Uptime & Convenience

- **Now –**

Security & Compliance

© Copyright 2016 Semel Consulting LLC ALL RIGHTS RESERVED – Slides and Cartoons may not be shared without permission

SEMEL CONSULTING

Patient Lawsuits

Then -

- **Medical Malpractice**
  - Medical Treatment
  - Complaint from 1 patient
  - Insurance coverage
  - Liability Limitations

Now -

- **Medical Malpractice**
  - Data Breach
  - Complaint from ALL patients at same time
  - Insurance coverage ???
  - Liability Limitations ???
- **Breach of Contract**
- **Negligent Misrepresentation**
  - Court considered Notice of Privacy Practices a contract with patients
  - Complaint from ALL patients at same time
  - Insurance ???

© Copyright 2016 Semel Consulting LLC ALL RIGHTS RESERVED – Slides and Cartoons may not be shared without permission

Recent News

Suffolk woman sentenced to more than 5 years in identity theft of patients

EX-UCLA HEALTHCARE EMPLOYEE SENTENCED TO FEDERAL PRISON FOR ILLEGALLY PEEKING AT PATIENT RECORDS

Healthcare IT News

Published in partnership with HIMSS

Six fired for keeping up with Kardashian

Renal & Urology News

Staff Nurse Faces Jail Time for HIPAA Violations

Respiratory Therapist Convicted in HIPAA Criminal Case

Prosecutors Alleged Patient Information Used to Seek Drugs

SEMEL CONSULTING

© Copyright 2016 Semel Consulting LLC ALL RIGHTS RESERVED – Slides and Cartoons may not be shared without permission

Recent News

County Government Settles Potential HIPAA Violations

$ 215,000 penalty

HEALTHCARE INFO SECURITY®

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.

SEMEL CONSULTING

© Copyright 2016 Semel Consulting LLC ALL RIGHTS RESERVED – Slides and Cartoons may not be shared without permission

Why Privacy & Confidentiality?

- Part of Patient Care
- HIPAA & Other Federal Laws
- State Data Breach Laws
- Employer Requirement
- Career Damage
- Nursing & Other Professional License Requirement
- Criminal Prosecution

© Copyright 2016 Semel Consulting LLC ALL RIGHTS RESERVED – Slides and Cartoons may not be shared without permission

SEMEL CONSULTING

Who Enforces HIPAA ?

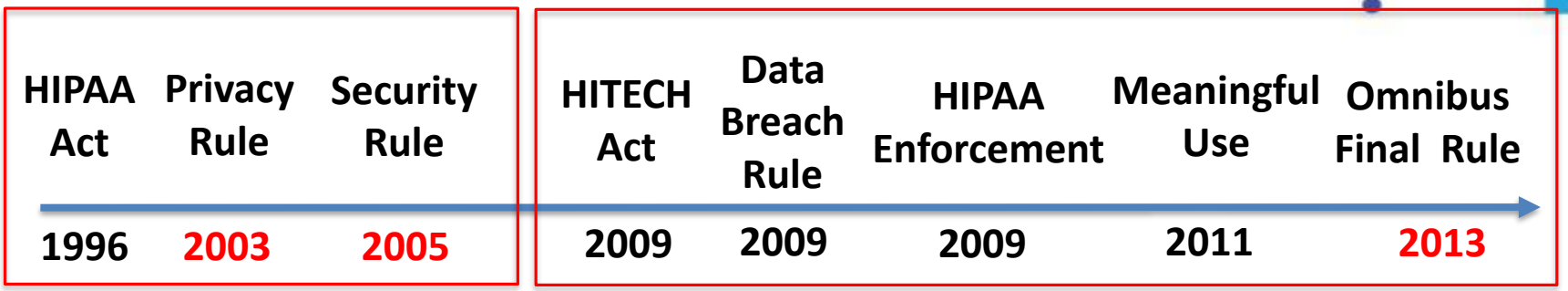
HHS Office for Civil Rights in Action

The US government treats Patient Privacy & Confidentiality as a Civil Right.
By violating HIPAA
you are violating Civil Rights.

© Copyright 2016 Semel Consulting LLC ALL RIGHTS RESERVED – Slides and Cartoons may not be shared without permission

SEMEL CONSULTING

HIPAA Timeline



- **Health Insurance Portability & Accountability Act** (1996)
  - **HIPAA Privacy Rule** (2003) **Protects ALL identifiable patient information – written, verbal, electronic (PHI)**
  - **Security Rule** (2005) **protects electronic Protected Health Information (ePHI) – over 50 requirements**
- **HITECH Act** (2009) **funded electronic medical records and changed HIPAA**
  - **Data Breach Rule** (2009) **sets reporting requirements & exemptions**
  - **HIPAA Omnibus Final Rule** released January, 2013
  - **COMPLIANCE DEADLINE – September 23, 2013**

© Copyright 2016 Semel Consulting LLC ALL RIGHTS RESERVED – Slides and Cartoons may not be shared without permission

SEMEL CONSULTING

HIPAA Fundamentals

- **Patient Privacy**
  - Can share info with caregivers
  - Cannot share info with others without specific authorization
  - Exclusions if unconscious or incompetent
- **Data Security**
  - Secure Systems – auto lockout, physical security
  - Unique User ID, password protection, encryption
- **Breach Reporting**
  - Timely patient notification, government notification

© Copyright 2016 Semel Consulting LLC ALL RIGHTS RESERVED – Slides and Cartoons may not be shared without permission

SEMEL CONSULTING

Orlando Shooting Aftermath

"The CEO of the hospital came to me and said they had an issue related to the families who came to the emergency room. Because of HIPAA regulations, they could not give them any information," *(Orlando Mayor Buddy) Dyer said.* ***"So I reached out to the White House to see if we could get the HIPAA regulations waived.*** *The White House went through the appropriate channels to waive those so the hospital could communicate with the families who were there."*

Source: WBTV.com

© Copyright 2016 Semel Consulting LLC ALL RIGHTS RESERVED – Slides and Cartoons may not be shared without permission

HIPAA doesn't interfere with patient care

- OK to share for **T**reatment, **P**ayment, and healthcare **O**perations (TPO) with other caregivers, payers, and business associates
- OK to share with patient's OK
- OK to verify patient's presence in ER
- OK to verify death
- OK to share with family & friends if patient is unconscious or incompetent - based on doctor's discretion
- OK to share with law enforcement to find fugitive or missing person, and for public safety
- Cannot share medical details with law enforcement

© Copyright 2016 Semel Consulting LLC ALL RIGHTS RESERVED – Slides and Cartoons may not be shared without permission

SEMEL CONSULTING

TPO

- **Covered Entities may share data with other CE's & Business Associates** for the purposes of **T**reatment, **P**ayment, and health care **O**perations
- **Treatment** – clinics, hospitals, doctors, specialists, pharmacies, labs, patient transfers, ambulance services,
- **Payment** – bills and correspondence to/from providers and payers
- Health Care **Operations** – Quality assessment, case management, training, accreditation

© Copyright 2016 Semel Consulting LLC ALL RIGHTS RESERVED – Slides and Cartoons may not be shared without permission

SEMEL CONSULTING

What is PHI & ePHI ?

- **Protected Health Information**
  - **Identifiable**

    (18 different identifiers)
  - **Plus treatment and/or diagnostic information**

- **Electronic Protected Health Information**
  - **PHI in electronic form**
  - **Words, images, voice files**
  - **On any media**

© Copyright 2016 Semel Consulting LLC ALL RIGHTS RESERVED – Slides and Cartoons may not be shared without permission

SEMEL CONSULTING

HIPAA IDENTIFIERS

1. **Names**

2. **All geographic subdivisions** smaller than a state, including street address, city, county, precinct, ZIP code, and their equivalent geocodes, except for the initial three digits of the ZIP code if, according to the current publicly available data from the Bureau of the Census:

(a) The geographic unit formed by combining all ZIP codes with the same three initial digits contains more than 20,000 people; and

(b) The initial three digits of a ZIP code for all such geographic units containing 20,000 or fewer people is changed to 000

3. All elements of dates (except year) for dates that are directly related to an individual, including birth date, admission date, discharge date, death date, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older

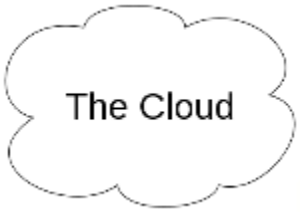
4. **Telephone numbers**
5. **Fax numbers**
6. **Email addresses**
7. **Social security numbers**
8. **Medical record numbers**
9. **Health plan beneficiary numbers**
10. **Account numbers**
11. **Certificate/license numbers**
12. **Vehicle identifiers and serial numbers, including license plate numbers**
13. **Device identifiers and serial numbers**
14. **Web Universal Resource Locators (URLs)**
15. **Internet Protocol (IP) addresses**
16. **Biometric identifiers, including finger and voice prints**
17. **Full-face photographs and any comparable images**
18. **Any other unique identifying number, characteristic, or code**, except as permitted by paragraph (c) of this section [Paragraph (c) is presented below in the section "Re-identification"]; and

(ii) The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

© Copyright 2016 Semel Consulting LLC ALL RIGHTS RESERVED – Slides and Cartoons may not be shared without permission

SEMEL CONSULTING

PHI & ePHI are EVERYWHERE



ANSWERING SERVICE

SEMEL CONSULTING

© ALL RIGHTS RESERVED – Slides and Cartoons may not be shared without permission

HIPAA Covers…

Covered Entities

Bill electronically

- Doctors
- Dentists
- Hospitals
- Skilled Nursing Facilities
- Pharmacies
- Health Plans

Business Associates

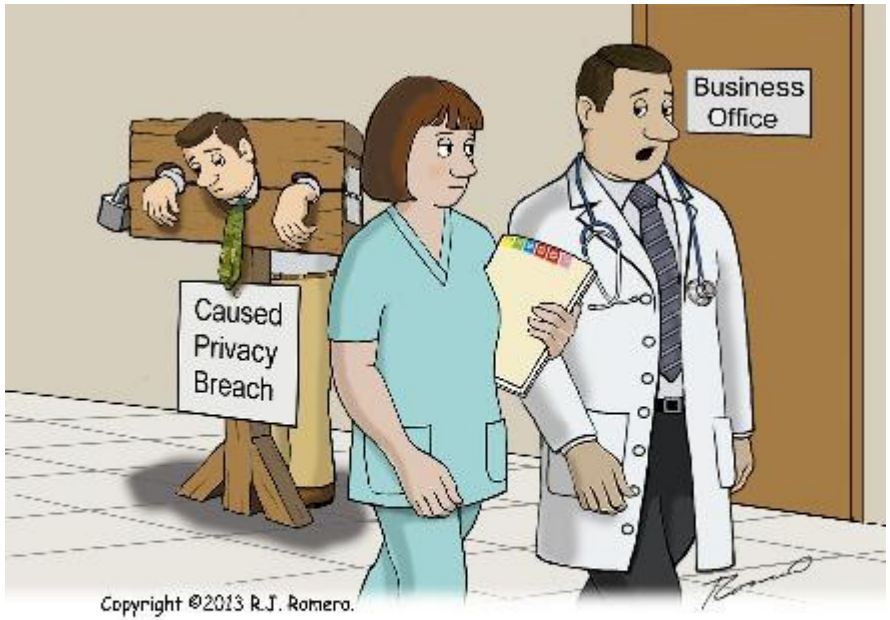
Maintain or Access PHI

- IT Companies
- EHR software
- Data Centers
- Cloud Vendors
- Paper Shredding
- Records Storage
- Copier Repair
- Billing
- Collections
- Healthcare org. lawyers
- Expert Witnesses
- Accountants
- Transcription

© Copyright 2016 Semel Consulting LLC ALL RIGHTS RESERVED – Slides and Cartoons may not be shared without permission

SEMEL CONSULTING

HIPAA Omnibus - Business Associates



That's our former attorney who thought HIPAA didn't apply to him because of attorney/client confidentiality."

- Must comply with HIPAA like Covered Entities – full programs
- Now clearly responsible for subcontractors
- Now includes more entities like data centers, cloud backup,
- New Business Associate Agreements

© Copyright 2016 Semel Consulting LLC ALL RIGHTS RESERVED – Slides and Cartoons may not be shared without permission

SEMEL CONSULTING

Not Business Associates

- **Conduits**
  - US Postal Service, Fedex, UPS
  - Internet Service Providers that only offer transport
- ***Incidental Contact with PHI***
  - *Janitorial Services*
  - *Contractors, repair men*

© Copyright 2016 Semel Consulting LLC ALL RIGHTS RESERVED – Slides and Cartoons may not be shared without permission

SEMEL CONSULTING

Compliance Responsibility

Patient

Covered Entity

Business Associate

Subcontractor Business Associate

IT Company

Online Backup

Data Centers

© Copyright 2016 Semel Consulting LLC ALL RIGHTS RESERVED – Slides and Cartoons may not be shared without permission

SEMEL CONSULTING

2016 HIPAA Audits

- 1,200 audits have started
- Will become permanent program
- Desk Audits – send in required documents
- Site Audits – on-site audits
- 10 days to respond
- Business Associates will also be audited
- If Business Associate fails, Covered Entity fails

© Copyright 2016 Semel Consulting LLC ALL RIGHTS RESERVED – Slides and Cartoons may not be shared without permission

SEMEL CONSULTING

176 HIPAA Audit Controls

http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol-current/index.html

2016 HIPAA Audit Protocol List

HIPAA PRIVACY RULE

1. Prohibited uses and disclosures - Use and disclosure of genetic information for underwriting purposes
2. Deceased individuals
3. Confidential communications
4. Uses and disclosures consistent with notice
5. Disclosures by whistleblowers
6. Disclosures by workforce members who are victims of a crime
7. Business associate contracts
8. Requirements for group health plans
9. Requirements for a covered entity with multiple covered functions
10. Permitted uses and disclosures
11. Consent for uses and disclosures
12. Authorizations for uses and disclosures is required
13. Compound authorizations – Exceptions
14. Prohibition on conditioning of authorizations
15. Uses and Disclosures for which an Authorization is Required – Documentation and Content
16. Use and Disclosure for Facility Directories; Opportunity to Object
17. Uses and Disclosures for Facility Directories in Emergency Circumstances
18. Permitted uses and disclosures
19. Uses and disclosures with the individual present
20. Limited uses and disclosures when the individual is not present
21. Uses and disclosures for disaster relief purposes
22. Uses and disclosures when the individual is deceased
23. Uses and disclosures required by law
24. Uses and disclosures for public health activities
25. Disclosures about victims of abuse, neglect or domestic violence
26. Uses and disclosures for health oversight activities
27. Disclosures for judicial and administrative proceedings
28. Disclosures for law enforcement purposes
29. Disclosures for law enforcement purposes - for identification and location
30. Disclosures for law enforcement purposes-- PHI of a possible victim of a crime
31. Disclosures for law enforcement purposes-- an individual who has died as a result of suspected criminal conduct
32. Disclosures for law enforcement purposes: crime on premises
33. Disclosures for law enforcement purposes
34. Uses and disclosures about decedents
35. Uses and disclosures for cadaveric organ, eye or tissue donation
36. Uses and disclosures for research purposes -- Permitted Uses and Disclosures
37. Uses and disclosures for research purposes -- Documentation of Waiver Approval
38. Uses and disclosures for specialized government functions -- Military
39. Uses and disclosures for specialized government functions -- National Security and intelligence activities
40. Uses and disclosures for specialized government functions -- Medical Suitability Determinations
41. Uses and disclosures for specialized government functions – Correctional institutions
42. Uses and disclosures for specialized government functions – Providing public benefits
43. Disclosures for workers' compensation
44. Requirements for De-Identification of PHI & Re-Identification of PHI
45. Minimum Necessary - Disclosures of PHI
46. Minimum Necessary requests for protected health information
47. Minimum Necessary - Other content requirement
48. Limited Data Sets and Data Use Agreements
49. Uses and Disclosures for Fundraising
50. Uses and Disclosures for Underwriting and Related Purposes
51. Verification Requirements
52. Notice of Privacy Practices Content requirements
53. Provisions of Notice - Health Plans
54. Provisions of Notice - Certain Covered Health Care Providers
55. Provision of Notice - Electronic Notice
56. Joint Notice by Separate Covered Entities
57. Documentation
58. Right of an Individual to Request Restriction of Uses and Disclosures
59. Terminating a Restriction
60. Documentation
61. Confidential Communications Requirements
62. Right to access
63. Denial of Access
64. Unreviewable grounds for denial
65. Reviewable grounds for denial
66. Review of denial of access
67. Documentation
68. Right to Amend
69. Denying the Amendment
70. Accepting the Amendment
71. Denying the Amendment
72. Right to an Accounting of Disclosures of PHI
73. Content of the Accounting
74. Provision of the Accounting
75. Documentation
76. Personnel designations
77. Training
78. Safeguards
79. Complaints to the Covered Entity
80. Complaints to the Covered Entity
81. Mitigation
82. Refraining from Intimidating or Retaliatory Acts
83. Waiver of rights
84. Policies and Procedures
85. Documentation

HIPAA SECURITY RULE

86. General Requirements
87. Flexibility of approach
88. Security Management Proce
89. Security Management Proce
90. Security Management Proce
91. Security Management Proce
92. Security Management Proce
93. Assigned Security Responsib
94. Workforce Security
95. Workforce security -- Autho
96. Workforce security -- Workf
97. Workforce security -- Establi
98. Information Access Manage
99. Information Access Manage
100. Information Access Manage
101. Information Access Manage
102. Security Awareness and Trai
103. Security Awareness and Trai
104. Security Awareness, Trainin
105. Security Awareness, Trainin
106. Security Awareness, Trainin
107. Security Incident Procedures
108. Security Incident Procedures
109. Contingency Plan
110. Contingency Plan – Data Bac
111. Contingency Plan –Disaster
112. Contingency Plan -- Emerge
113. Contingency Plan -- Testing
114. Contingency Plan --Applicati
115. Evaluation
116. Business Associate Contract
117. Business Associate Contract
118. Facility Access Controls
119. Facility Access Controls -- Co
120. Facility Access Controls -- Fa
121. Facility Access Controls -- Ac
122. Facility Access Controls -- M
123. Workstation Use
124. Workstation Security
125. Device and Media Controls
126. Device and Media Controls -
127. Device and Media Controls -- Media Re-use
128. Device and Media Controls – Accountability
129. Device and Media Controls -- Data Backup and Storage Procedures
130. Access Control
131. Access Control -- Unique User Identification
132. Access Control -- Emergency Access Procedure
133. Access Control -- Automatic Logoff
134. Access Control -- Encryption and Decryption
135. Audit Controls
136. Integrity
137. Integrity -- Mechanism to Authenticate ePHI

71 Data Security Auditable Items

© Copyright 2016 Semel Consulting LLC ALL RIGHTS RESERVED – Slides and Cartoons may not be shared without permission

SEMEL CONSULTING

HIPAA Myths & Facts

Myth: HIPAA is about compliance

- **HIPAA is about patient privacy and preventing data breaches**

Myth: "I need to have a HIPAA Risk Analysis."

- **You need a Risk Analysis and you must mitigate the risks you identify and be compliant**

Business Associate Myth: "We're compliant. We signed a Business Associate Agreement."

- **Every Business Associate and their subcontractors must have a comprehensive compliance program**

© Copyright 2016 Semel Consulting LLC ALL RIGHTS RESERVED – Slides and Cartoons may not be shared without permission

SEMEL CONSULTING

Notice of Privacy Practices
PHI Release Authorization

- Required for Providers and Payers, not BA's
- NPP summarizes how patient data is used & shared
- PHI release limited to specific PHI, for specific use, with Expiration date
- Modified by Omnibus Rule to now include electronic records and certain types of marketing activities
- Must be posted prominently in waiting area and on website

© Copyright 2016 Semel Consulting LLC ALL RIGHTS RESERVED – Slides and Cartoons may not be shared without permission

SEMEL CONSULTING

Encryption

- Higher level of security than passwords
- Locks data in secure container that requires a key to unlock data
- If device is stolen or drive is removed data cannot be accessed
- Encrypted data is not reportable under HIPAA or state data breach laws (as long as encryption key isn't breached)
- No-brainer

© Copyright 2016 Semel Consulting LLC ALL RIGHTS RESERVED – Slides and Cartoons may not be shared without permission

SEMEL CONSULTING

FBI Warning to Healthcare

The biggest vulnerability *(to the security of patient data)* ***was the perception of IT healthcare professionals' beliefs that their current perimeter defenses and compliance strategies were working*** *when clearly the data states otherwise.*

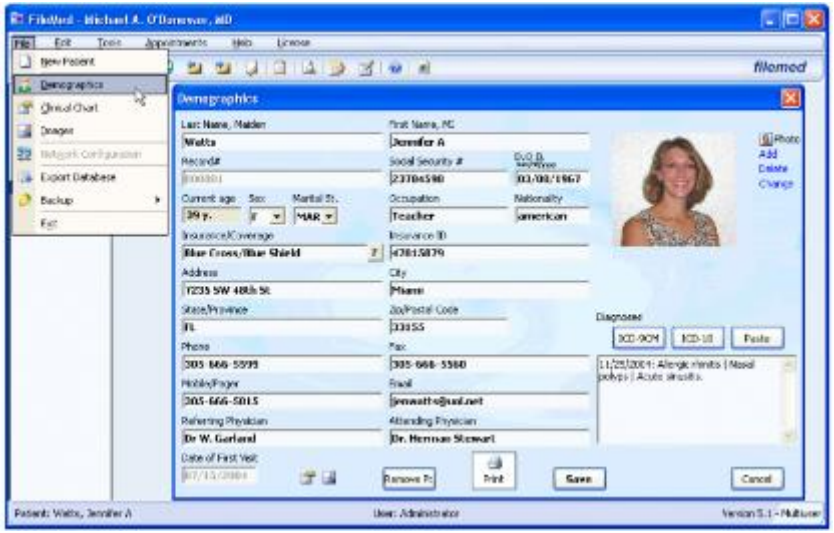
© Copyright 2016 Semel Consulting LLC ALL RIGHTS RESERVED – Slides and Cartoons may not be shared without permission

SEMEL CONSULTING

Medical Record Black Market

- Credit Card Number

25¢ - $1



- Medical Record

$10 - $50

UNCLASSIFIED

FBI CYBER DIVISION

Private Industry Notification

SEMEL CONSULTING

© Copyright 2016 Semel Consulting LLC ALL RIGHTS RESERVED – Slides and Cartc

2016 Cost of a Data Breach Report

- $ 221 per record across all industries
- $ 402 per record for health care breaches

- 10,000 records x $ 402 = $ 4,020,000
- 25,000 records x $ 402 = $ 10,050,000
- 100,000 records x $ 402 = $ 40,200,000

Source: Ponemon Institute

© Copyright 2016 Semel Consulting LLC ALL RIGHTS RESERVED – Slides and Cartoons may not be shared without permission

SEMEL CONSULTING

Data Breach Enforcement

"Somehow your medical records got faxed to a complete stranger. He has no idea what's wrong with you either."

© Copyright 2016 Se

SEMEL CONSULTING

HIPAA Data Breach Law

- Breaches over 500 records report within 60 days
  - Posted on public website
- Breaches under 500 records report annually
- Patients must be notified
- No longer a harm exemption
- All losses presumed to be a breach
  - Minor exceptions
- Encrypted devices exempt from reporting

© Copyright 2016 Semel Consulting LLC ALL RIGHTS RESERVED – Slides and Cartoons may not be shared without permission

SEMEL CONSULTING

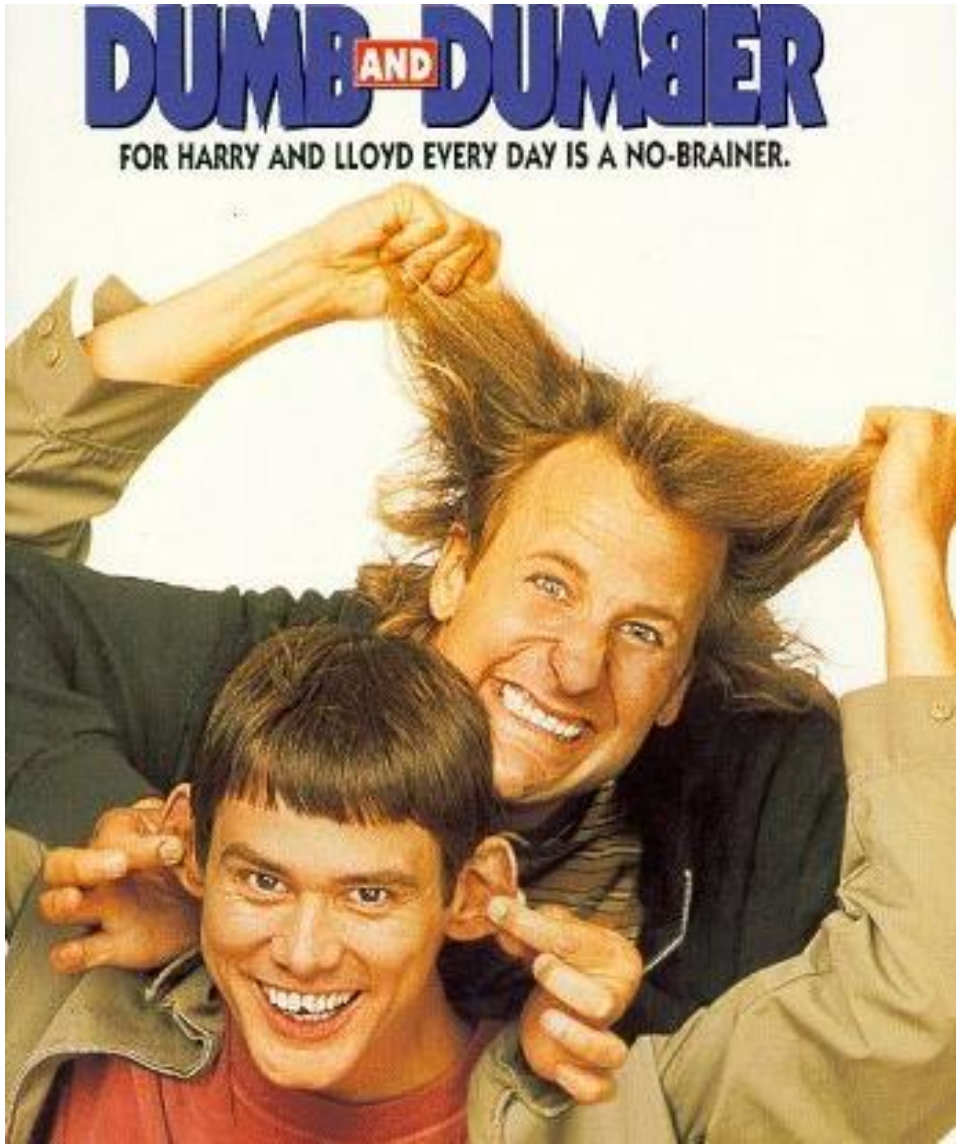
OCR Penalties

- **$ 100,000** – 5-doctor practice in Phoenix for sending PHIby unsecure e-mails
- **$ 1.7 million – Alaska state health dept. lost backup drive**
- **$ 1.5 million** – Massachusetts hospital stolen laptop
- **$ 400,000** – university clinic failed firewall
- **$ 1.2 million – data left on copier hard drives at end of lease**
- **$ 150,000 – lost thumb drive**
- **$ 1.7 million – lost unencrypted laptop, was listed in Risk Analysis**
- **$ 4.8 million** – two NYC hospitals – doctor used own server & published patient info to Internet
- **$ 150,000 – Non-profit mental health clinic – no firewall/unsupported software**
- **$ 750,000** – small cancer radiology group – stolen bag with laptop & backup media
- **$ 750,000 – ortho clinic – sharing PHI without a Business Associate Agreement**
- **Plus costs to notify patients & remediate problems**
- **Publication on the HIPAA 'Wall of Shame'**

SEMEL CONSULTING

© Copyright 2016 Semel Consulting LLC ALL RIGHTS RESERVED – Slides and Cartoons may not be shared without permission

HIPAA Violations



© Copyright 2016 Semel Consulting LLC ALL RIGHTS RESERVED – Slides and Cartoons may not be shared without permission

SEMEL CONSULTING

Dumb Shasta Regional Medical Center

- Hospital accused of Medicare Fraud
- Patient fell
- Hospital billed Medicare for malnutrition treatment, double the cost of a simple fall
- Patient showed local newspaper some of her medical record
- The hospital president & CMO took the patient's chart to the local newspaper & shared info with the LA Times

© Copyright 2016 Semel Consulting LLC ALL RIGHTS RESERVED – Slides and Cartoons may not be shared without permission

SEMEL CONSULTING

Headlines, Reprimand, & Fine

Los Angeles Times

Her case shows why healthcare privacy laws exist

"an individual's PHI remains protected even when it has been disclosed by the individual herself or otherwise made a part of the public record and that disclosures of PHI to the media always require the patient's authorization."

$ 275,000 fine

© Copyright 2016 Semel Consulting LLC ALL RIGHTS RESERVED – Slides and Cartoons may not be shared without permission

SEMEL CONSULTING

Dumber – NY Presbyterian Hospital

- Hospital Allowed NY MED TV crew to film 2 patients – one dying and the other in severe distress- without permission
- Even after a doctor asked them to stop

© Copyright 2016 Semel Consulting LLC ALL RIGHTS RESERVED – Slides and Cartoons may not be shared without permission

SEMEL CONSULTING

Headlines, Reprimand, & Fine

The New York Times

New York Hospital to Pay $2.2 Million Over Unauthorized Filming of 2 Patients

"It is not sufficient for a health care provider to request or require media personnel to mask the identities of patients (using techniques such as blurring, pixelation or voice alteration software) for whom an authorization was not obtained," the Office for Civil Rights with the federal Department of Health and Human Services said

$ 2,200,000 fine

© Copyright 2016 Semel Consulting LLC ALL RIGHTS RESERVED – Slides and Cartoons may not be shared without permission

SEMEL CONSULTING

Training
Snooping
E-mail & Texting
Logins & Passwords

© Copyright 2016 Semel Consulting LLC ALL RIGHTS RESERVED – Slides and Cartoons may not be shared without permission

SEMEL CONSULTING

Training - Required

- **All Workforce Members** must receive HIPAA training prior to accessing records
  - Employees, Contractors, Volunteers, Students
- **Annual Refresher**
- **Keep detailed records for all workforce members**
- **Include students, part-timers, contractors, temps, volunteers**
- **Managers should understand HIPAA rules**
- **Employees should know what to do/not to do**

© Copyright 2016 Semel Consulting LLC ALL RIGHTS RESERVED – Slides and Cartoons may not be shared without permission

SEMEL CONSULTING

Snooping is Forbidden

- **HIPAA Minimum Access Requirement**
  - Educate workforce
  - EHR – limit access by job role
  - Network – limit access by job role
- **No viewing of records unless you need to**
- **No viewing your own record, family, friends, neighbors, celebrities**
- **EHR Systems log access**

© Copyright 2016 Semel Consulting LLC ALL RIGHTS RESERVED – Slides and Cartoons may not be shared without permission

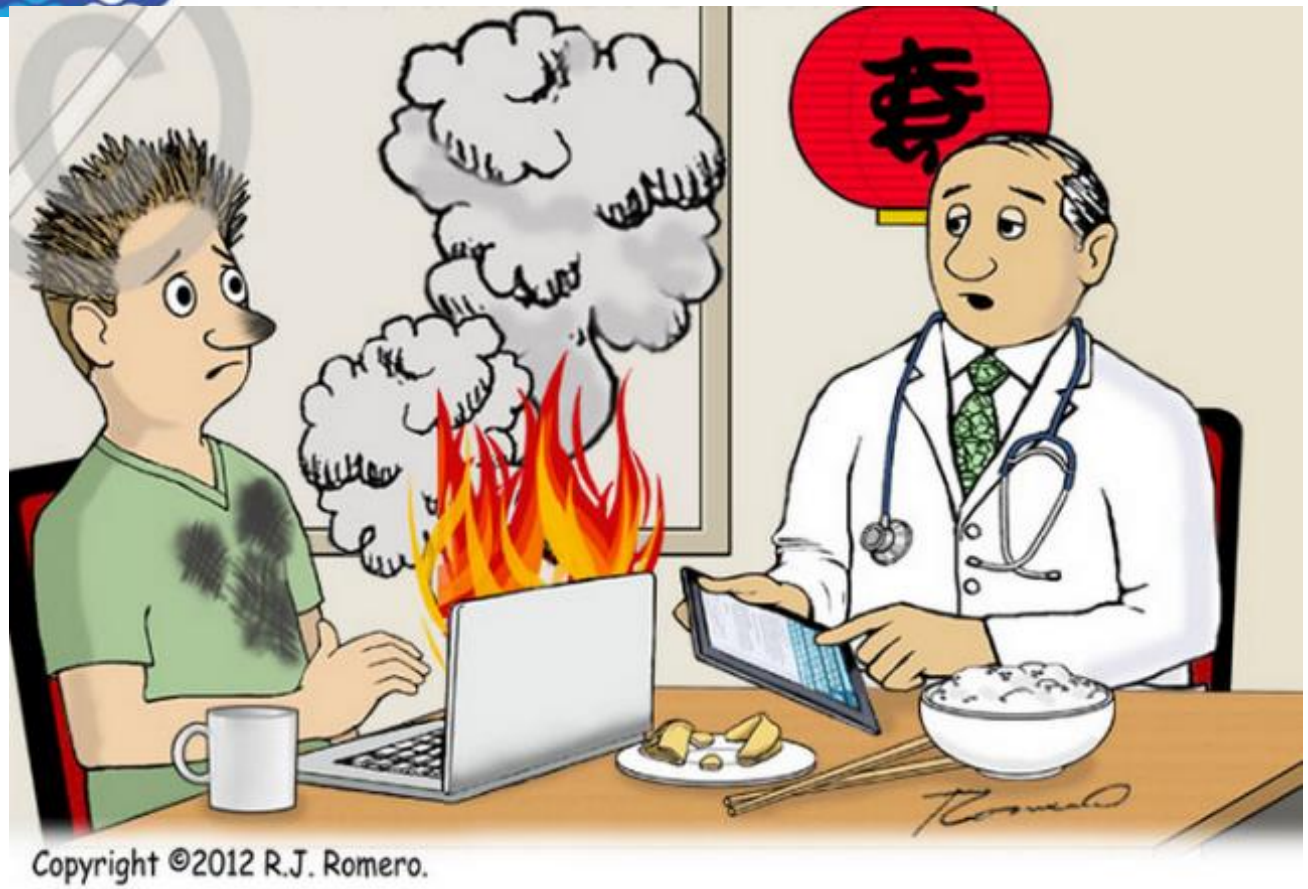
SEMEL CONSULTING

HIPAA Outlives You by 50 years

© Copyright 2016 Semel Consulting LLC ALL RIGHTS RESERVED – Slides and Cartoons may not be shared without permission

SEMEL CONSULTING

Technology



© Copyright 2016 Semel Consulting LLC ALL RIGHTS RESERVED – Slides and Cartoons may not be shared without permission

SEMEL CONSULTING

More than Technology Tools

© Copyright 2016 Semel Consulting LLC ALL RIGHTS RESERVED – Slides and Cartoons may not be shared without permission

SEMEL CONSULTING

E-mail – Must be Secure

- **No Free E-mail services**
- **Must use secure e-mail system**
  - Within practice
  - Encrypt PHI outside of practice or use patient portal for communications
  - **Exception if patient requests records be sent to their webmail account**
    - Warn that webmail is not secure
    - Document patient authorization
  - Manage smart phones

© Copyright 2016 Semel Consulting LLC ALL RIGHTS RESERVED – Slides and Cartoons may not be shared without permission

SEMEL CONSULTING

Texting

- No PHI in text messages
- Can have patient name but no medical info
- Can have medical info but no patient name
- Best to send message to call for details

OK to Send

Please call Mr. Smith at _____

The labs you requested are ready.

Please call about Mr. Smith.

Mr. Smith needs a new prescription.

© Copyright 2016 Semel Consulting LLC ALL RIGHTS RESERVED – Slides and Cartoons may not be shared without permission

Logins & Passwords

- **Every User Must Have Unique User ID**
  - No Shared ID's
  - For Network & EHR system
- **Every Password Must Be Secure**
  - No Shared Passwords
  - Strong Passwords
  - Passwords changed every 60 – 90 days
  - More often with high risk IT or staff changes
  - Hidden

© Copyright 2016 Semel Consulting LLC ALL RIGHTS RESERVED – Slides and Cartoons may not be shared without permission

SEMEL CONSULTING

Security & Compliance

© Copyright 2016 Semel Consulting LLC ALL RIGHTS RESERVED – Slides and Cartoons may not be shared without permission

SEMEL CONSULTING

Why Executive Responsibilities ?

© Copyright 2016 Semel Consulting LLC ALL RIGHTS RESERVED – Slides and Cartoons may not be shared w

- **Compliance Assessments**
- **Meaningful Use Security Risk Analysis**
- **Outsourced Security Officer Services**
- **HIPAA Compliance Remediation**
- **Work with practice & IT staff/provider**

Mike Semel

mike@semelconsulting.com

888-997-3635 x101

© Copyright 2016 Semel Consulting LLC ALL RIGHTS RESERVED – Slides and Cartoons may not be shared without permission

SEMEL CONSULTING