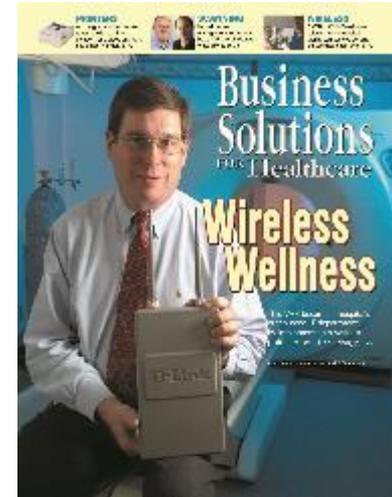


**You Think You Are Secure,  
But Can You Pass  
a Compliance Audit  
Or  
Data Breach Investigation  
???**

# 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 Plus (holder, development team, author- quick reference guide, coach)



## Mike Semel

President  
Chief Compliance Officer  
SEMEL Consulting



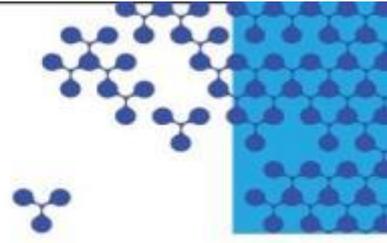
# Rose Ketchum



- **VP, Business Development**
- **30-year IT industry**
- **Certified HIPAA Security Professional**



# DEFINITION: Security



Security is...

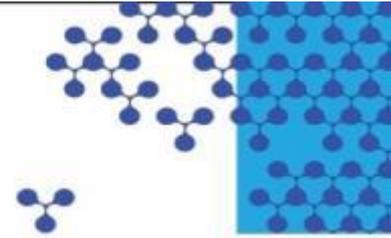
**The protection of data against...**

**LOSS,**

**THEFT,**

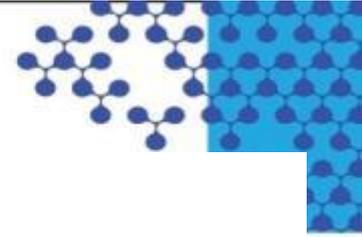
**and UNAUTHORIZED ACCESS.**

# How to Approach Security



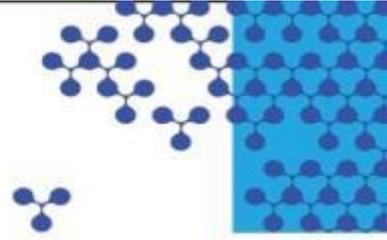
**Security is a BUSINESS problem  
With a TECHNICAL solution**

# DEFINITION: Compliance



- **Having to meet requirements set by others**
  - **Governments – federal & state**
    - HIPAA, GLBA, FFIEC, SEC, FDIC, NCUA, FISMA, CIPA, FERPA, E-Rate, State Breach Laws, State Agency Requirements
  - **Industry**
    - PCI-DSS, Bar Association Ethics Requirements
  - **Insurance Companies**
    - Application Requirements
  - **Client Requirements**
    - Contract Requirements
- **Cyber Security Controls**
- **Data Breach Prevention / Response / Reporting**

# Definition: Audits - Investigations



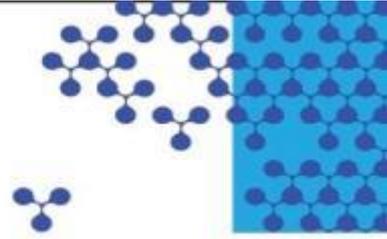
- **Audits**

- Proactive
- Random
- Desk Audits
- Site Audits

- **Data Breach Investigations**

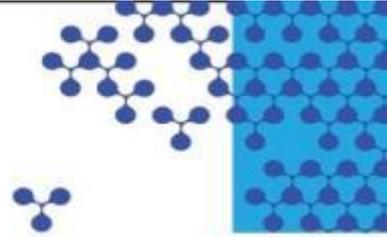
- Reactive
- Triggered by Known or Suspected Breach, or Allegation

# First Question after Data Breach



How did our  
IT department  
#&%%! up to  
cause this to  
happen  
????!!!!

# Public Sector Data Breach

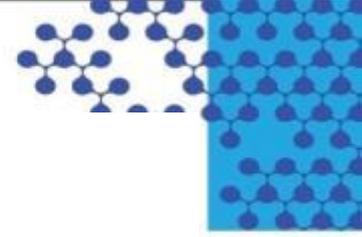


- **Media**
- **Politicians**
- **Public**

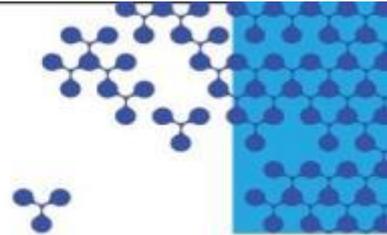
# What does the person talking to the public know about computers?



# CIO – IT Director Scapegoat



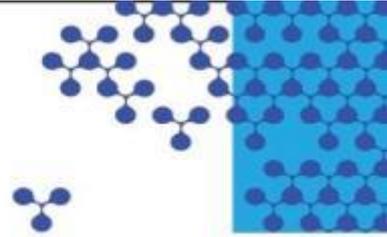
# Regulatory Compliance Examples



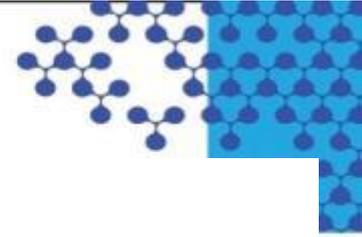
- **HIPAA** – applies to health care providers, health plans (including self-funded) & Business Associates that provide services to health care organizations
- **State Data Breach Laws** – protect Social Security & Driver's License Numbers
- **Cyber Liability Insurance** Policy Requirements
- **Contracts**

# HIPAA Fundamentals

- **Patient Privacy**
- **Data Security**
  - Secure Systems – auto lockout, physical security
  - Unique User ID, password protection, encryption
- **Breach Reporting**
  - Timely patient notification, government notification

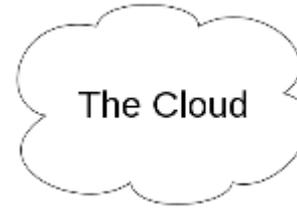
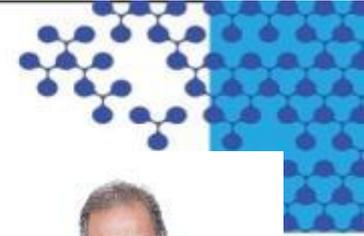


# What is PHI & ePHI ?



- **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**

# PHI & ePHI are EVERYWHERE



**ANSWERING SERVICE**

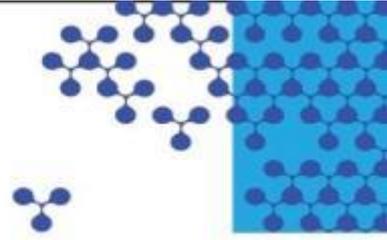


# FBI Warning to Healthcare

*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.*



# 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

# 176 HIPAA Audit Controls

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

## 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

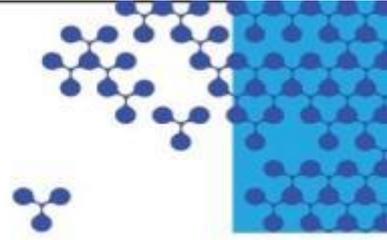
## HIPAA SECURITY RULE

86. General Requirements
87. Flexibility of approach
88. Security Management Process
89. Security Management Process
90. Security Management Process
91. Security Management Process
92. Security Management Process
93. Assigned Security Responsibility
94. Workforce Security
95. Workforce security - Authentication
96. Workforce security - Workstation Security
97. Workforce security - Establishment of Information Access Management
98. Information Access Management
99. Information Access Management
100. Information Access Management
101. Security Awareness and Training
102. Security Awareness and Training
103. Security Awareness, Training
104. Security Awareness, Training
105. Security Awareness, Training
106. Security Awareness, Training
107. Security Incident Procedures
108. Security Incident Procedures
109. Contingency Plan
110. Contingency Plan - Data Backup
111. Contingency Plan - Disaster Recovery
112. Contingency Plan - Emergency
113. Contingency Plan - Testing
114. Contingency Plan - Application
115. Evaluation
116. Business Associate Contract
117. Business Associate Contract
118. Facility Access Controls
119. Facility Access Controls - Configuration
120. Facility Access Controls - Functionality
121. Facility Access Controls - Access
122. Facility Access Controls - Management
123. Workstation Use
124. Workstation Security
125. Device and Media Controls
126. Device and Media Controls - Disposal
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

138. Person or Entity Authentication

# 71 Data Security Auditable Items

# 71 HIPAA Data Security Audit Controls



## Examples

**Password Expiration**

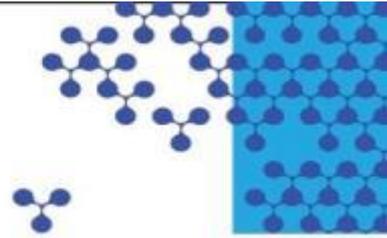
**Unique User Identification**

**No Terminated Users with Access  
Systems with Supported Software**

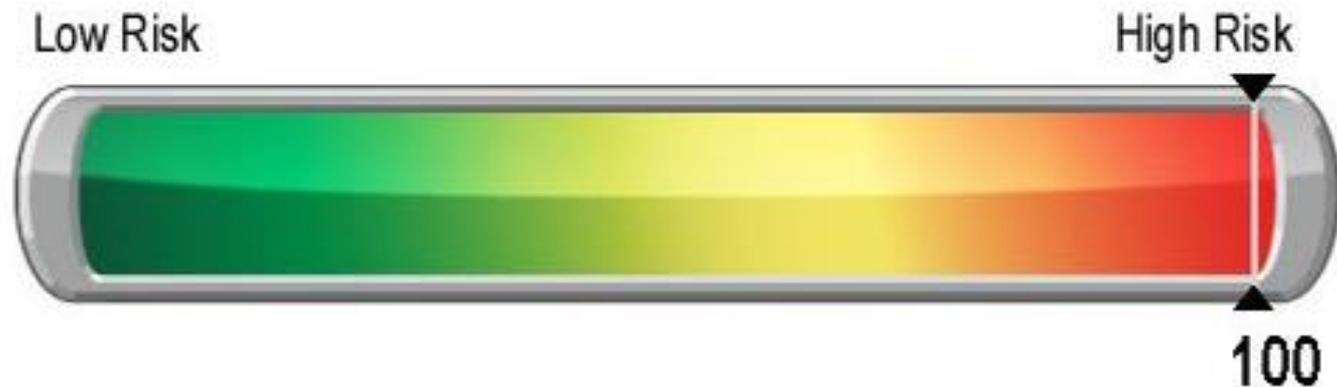
**Current Patches & Updates**

**Data Backed Up Offsite**

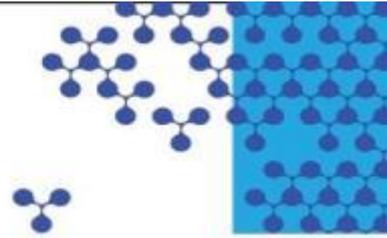
# CIO: “We have Security handled”



## Network Assessment Scan

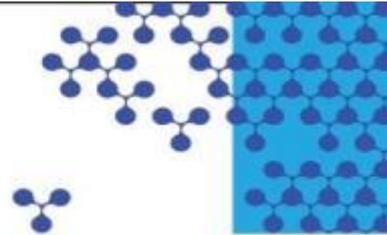


# Questionnaire



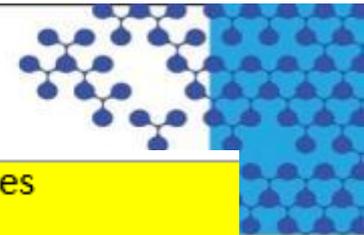
Passwords	Answer / Comment / Is document attached?
Are individual logins required to your network? To your application?	Yes, Yes
Are any generic logins used for your network or application? (nurse, Exam Room 1, etc.)	Only for some station assigned Instant Messaging
How frequently must passwords be changed?	90 days
Is re-using a previous password prohibited?	Yes
Are strong passwords required?	Yes
Is the system set to lock out users after no more than 5 failed login attempts?	Yes
Are all user passwords changed immediately upon the termination of an IT support technician or other high risk employee?	yes
Are managers set up to access their employee's passwords without asking the employee for their password?	No
Are any logins and passwords written down and visible near users?	No, per policy, but it is possible
List any users exempt from password rules.	No one

# Network Scan Results - Passwords



User Name	Display Name	Password Last Set	Password Expires	Last Login
		7/25/2013 11:47:02 AM	<never>	11/17/2015 8:37:52 AM
		5/1/2013 11:41:30 AM	<never>	12/9/2015 12:22:48 PM
		9/23/2013 5:11:34 PM	<never>	12/4/2015 9:08:49 AM
		5/31/2013 4:10:19 PM	<never>	<never>
		6/11/2013 2:46:40 PM	<never>	12/9/2015 11:50:10 AM
		8/29/2013 9:04:48 AM	<never>	12/8/2015 3:42:54 PM
		6/5/2013 8:30:53 AM	<never>	12/3/2015 1:18:15 PM
		2/11/2003 10:33:01 AM	<never>	11/19/2015 12:13:11 PM
		12/3/2008 3:09:35 PM	<never>	<never>

# Questionnaire

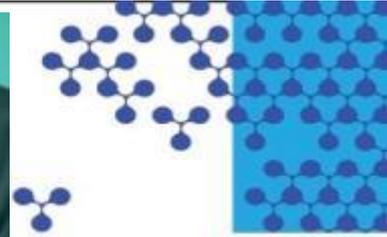


Are patches and updates installed on all computers and servers? PLEASE SEND A REPORT DETAILING YOUR SYSTEMS AND THEIR PATCH/UPDATE STATUS	Yes
Is patching and updating manual or automatic?	Automatic

## Network Assessment Scan Results - Patches

Updates, Windows Server 2008 R2	Failed (non-critical)	33 updates are missing.
<b>Critical Updates, Windows Server 2008</b>	<b>Failed (critical)</b>	<b>4 critical updates are missing.</b>
Feature Packs, Silverlight	Failed (non-critical)	1 update is missing.
Feature Packs, Windows Live	Failed (non-critical)	1 update is missing.
Feature Packs, Windows Server 2008	Failed (non-critical)	1 update is missing.
<b>Security Updates, Visual Studio 2005</b>	<b>Failed (critical)</b>	<b>1 security update is missing.</b>
<b>Security Updates, Visual Studio 2010</b>	<b>Failed (critical)</b>	<b>1 security update is missing.</b>
<b>Security Updates, Windows Server 2008</b>	<b>Failed (critical)</b>	<b>104 security updates are missing.</b>
Update Rollups, Windows Server 2008	Failed (non-critical)	1 update is missing.
Updates, Windows Server 2008	Failed (non-critical)	10 updates are missing.

# OCR Penalties



- \$ 100,000 – 5-doctor practice in Phoenix for sending PHI by 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’

# Lawsuits



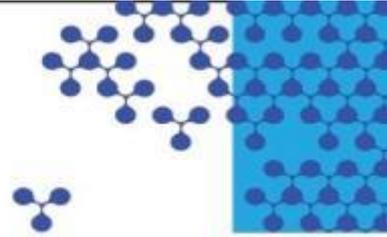
## Then -

- **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 ???

# Cyber Liability Insurance



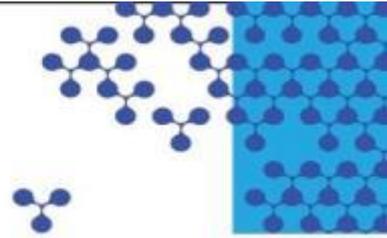
## Insurer Seeks Breach Settlement Repayment

Alleges Client Failed to Follow 'Minimum Practices'

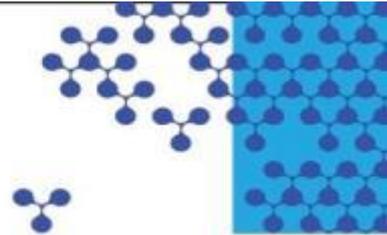
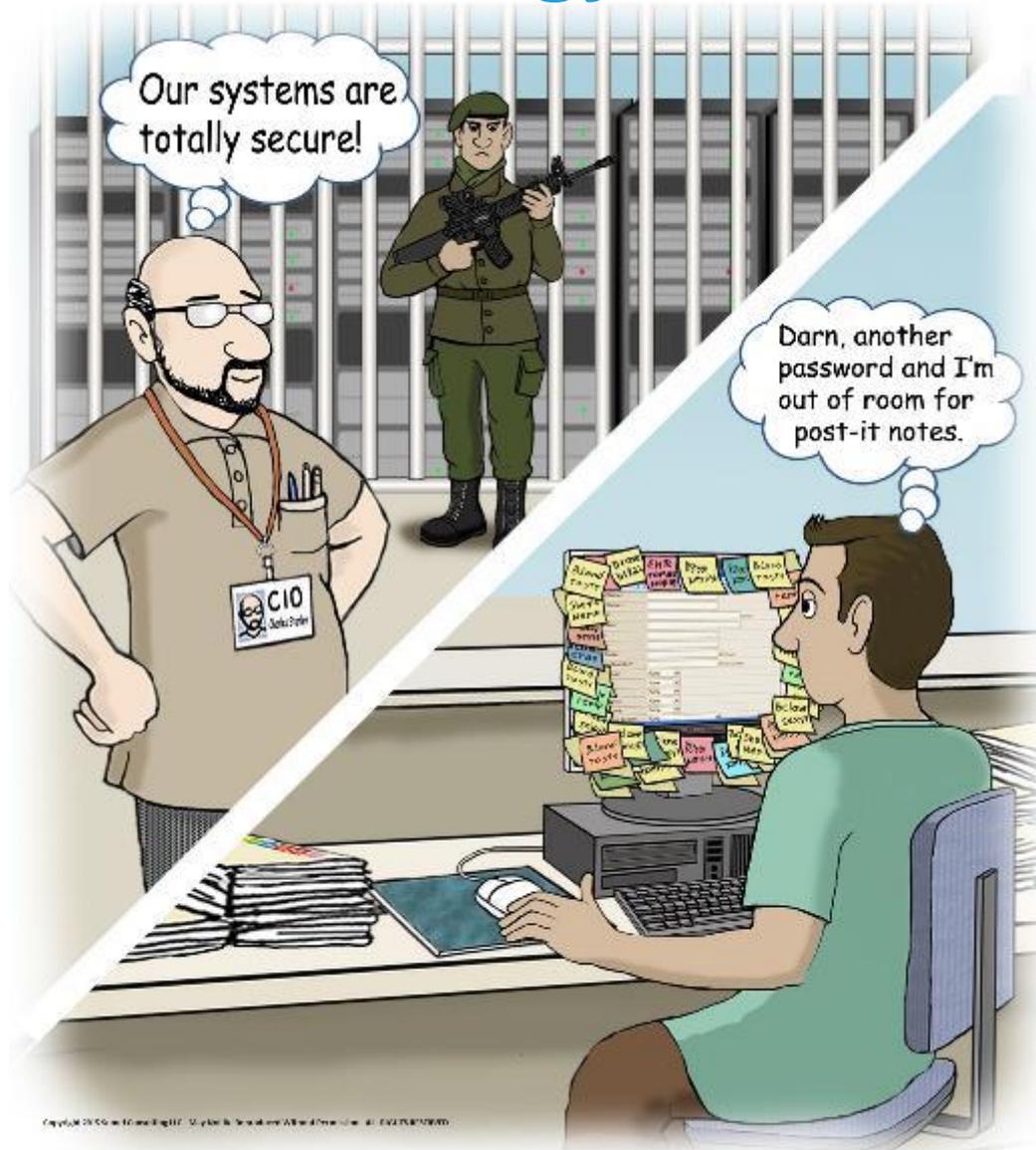
**Columbia Casualty alleges that Cottage Health's application for coverage under the Columbia policy "contained misrepresentations and/or omissions of material fact that were made negligently or with intent to deceive concerning Cottage's data breach risk controls," according to the insurer's lawsuit.**



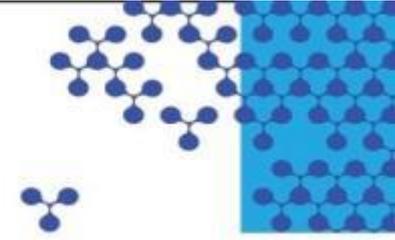
# Security & Compliance



# More than Technology Tools



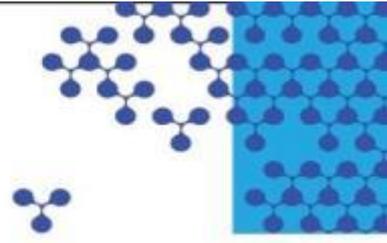
# How to Manage Compliance



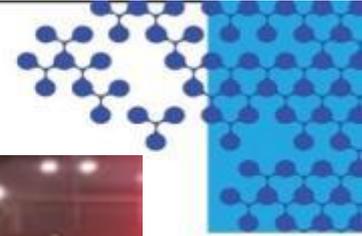
- **Understand Compliance Regulations**
- **Pay Attention to the Details**
  - Review Reports
  - Check Devices
  - Demand appropriate documentation
- **Trust but Verify**
- **Get Independent Opinion**
- Repeat

# How to Get Budget

- **Tie technology to business needs**
  - School District receives \$ 1 million E-Rate Funding
  - E-Rate requires compliance with Children's Internet Protection Act (CIPA)
  - CIPA compliance required \$ 50,000 in new firewalls
  - School Board Presentation connected the dots
- “To protect our \$ 1 million E-Rate funding we only need to spend \$ 50,000 on firewalls.”
- Immediate vote to purchase firewalls



# Security is Mostly People



<https://www.youtube.com/watch?v=opRMrEfAlil>



SEMEL  
CONSULTING

# HIPAA SOS

SECURITY OFFICER SERVICES

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

Mike Semel – [mike@semelconsulting.com](mailto:mike@semelconsulting.com) 888-997-3635 x101

