Welcome!

Cerebral Palsy Associations of New York State

Real people. Realizing potential.

NY SHIELD Act CRITICAL ACTION STEPS & DEADLINES for CP of NYS Affiliates

This is not legal advice. It is your responsibility to evaluate the accuracy, completeness and usefulness of any information, opinion or content and to seek appropriate advice of professionals, as appropriate.

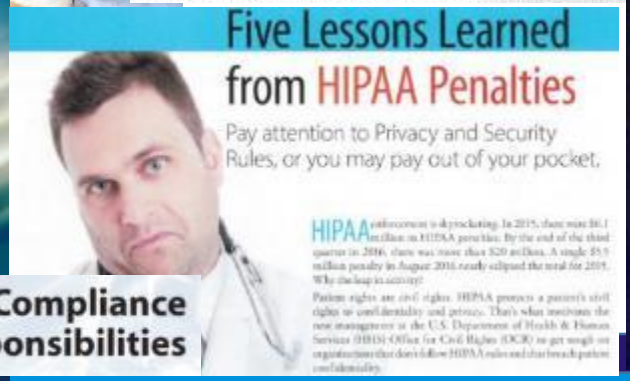
SEMEL CONSULTING

Mike Semel

- 40-year IT business owner/manager
- 17-year certified HIPAA Professional
- EMT/ER Tech/FD Rescue Captain /IndyCar Safety Team
- Hospital/Skilled Nursing CIO
- School District CIO
- Cloud Backup Service COO
- HIPAA Courseware author

Mike Semel
President
Chief Compliance Officer
SEMEL Consulting

Speaking, Writing

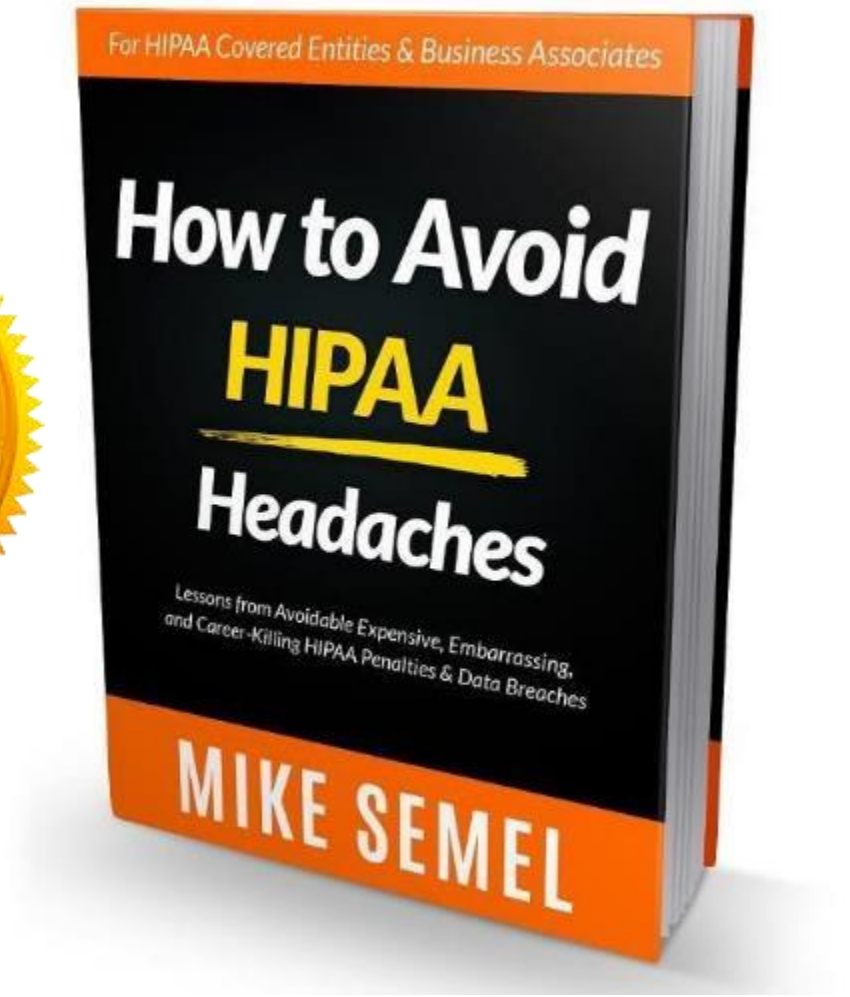


Why Security and Compliance Are Executive Responsibilities

SEMEL CONSULTING

2019 Quality & Compliance Conference

Amazon Best-Seller



A DATA BREACH HORROR STORY

Patient Data Published to Internet

- **Cottage Health's IT company accidently published a server to the Internet**
- **Patients Googled Themselves & Got Their Medical Records**
- The IT company did not have insurance so Cottage Health filed a claim with its cyber-liability carrier, Columbia Casualty
- **Patients sued, 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.

SEMEL CONSULTING

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

- 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

What is Compliance?

Having to meet requirements set by others

- Federal & State Laws
- Industry Regulations
- Contractual Obligations
- Insurance Policy Requirements

Security & Compliance

It’s not about what you do.

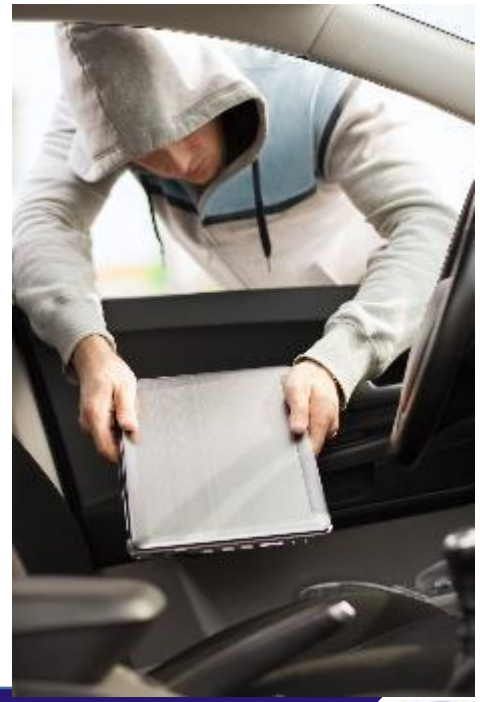
It’s all about what you can prove you do in writing, to respond to regulators & lawsuits.

HIPAA

- **Privacy Rule**
  - **Protect all Identifiable Medical Information**
  - **Minimum Necessary Access** (no snooping in records without a business reason)
- **Security Rule**
  - **Framework of security requirements**
  - **Business Associate vendor relationships**

HIPAA Breach Notification Rule

- **Breach**
  - **Loss, theft, or unauthorized access of unencrypted PHI**
  - **Individual Notification**
    - As soon as possible, no more than 60 days
    - Media notice and additional requirements for breaches of more than 500 records
  - **Government Reporting for ALL breaches**
    - Under 500 records – annual report due 60 days after year-end
    - Over 500 records – within 60 days
    - Online reporting portal



HIPAA Breach Notification Rule Exceptions

- …**presumed to be a breach** unless the covered entity or business associate, as applicable, **demonstrates** that there is a **low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:**
  - The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
  - The unauthorized person who used the protected health information or to whom the disclosure was made;
  - Whether the protected health information was actually acquired or viewed; and
  - The extent to which the risk to the protected health information has been mitigated.

THESE ARE NARROW EXCEPTIONS - NOT BIG LOOPHOLES

Current NY State Breach Law

- **Protects the following data if <u>acquired</u> without authorization**
  - **Social Security Number**
  - **Driver's License or non-driver ID**
  - **Account number, credit card number, or debit card number** in combination **with any required security code, access code, or password** that would permit access to an individual's financial account.

IMPORTANCE TO CP Affiliates:
INDIVIDUALS – SS# AND BANK ACCOUNT INFO
HR RECORDS OF APPLICANTS, CURRENT EMPLOYEES, FORMER EMPLOYEES; CURRENT AND PAST CONTRACTORS; VEHICLE ACCIDENT REPORTS

NY State Penalties

Attorney General
Barbara D. Underwood

A.G. Underwood Announces $200,000 Settlement With Buffalo Non-Profit For Exposing Clients' Sensitive Personal Information On Internet For Years

NY Attorney General HIPAA Fine for URMC

12-Month Suspension for Nurse Who Provided Patient Information to New Employer

NY SHIELD Act – consumer protection

- **S**top **H**acks and **I**mprove **E**lectronic **D**ata **Security** Act
  - Signed into law July 25, 2019
  - Breach notification requirements go into effect October 23, 2019
  - Data security requirements go into effect March 21, 2020
- **Applies to all businesses that store data about New Yorkers**
- **Expands definition of Private Information**
- **Changes breach to include 'access' to data instead of just 'acquiring' data**
- **Requires reasonable data protection**
- **Failure considered an unfair business practice**
- **Exemptions for regulated businesses**

NY SHIELD Act – consumer protection

- **Private Information**
  - Unencrypted, or encrypted with encryption key
- **Expands definition of Private Information**
  - Biometrics
  - Username & password to online account
  - Account number, or credit or debit card number, even without compromise of an access code or password, is reportable, "if circumstances exist wherein such number could be used to access an individual's financial account without additional identifying information, security code, access code, or password."
- **Changes breach to include 'access' to data instead of just 'acquiring' data**
- **Requires reasonable data protection**
- **Failure considered an unfair business practice**

Unauthorized Access

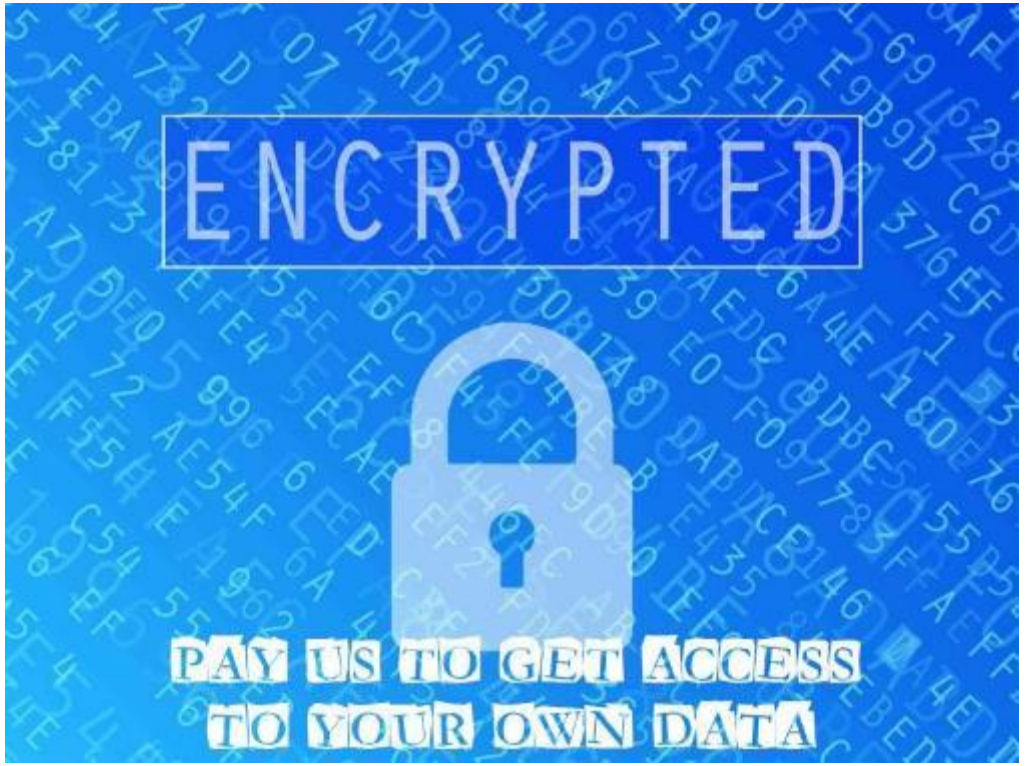
*"**indications that the information was viewed**, communicated with, **used**, or altered **by a person without valid authorization** or by an unauthorized person."*

- Exemption for "good-faith employee" access
- No exemption for access by an employee with bad intentions

NY SHIELD Act – Ransomware?

Factors for determining if a breach has occurred:

- *"indications that the information was viewed, communicated with, used, **or altered** by a person without valid authorization or by an unauthorized person."*



NY SHIELD Act – Other Compliance Laws

- **Businesses that are already regulated by and comply with data breach notice requirements** HIPAA, NY DFS Reg 500, Gramm-Leach-Bliley Act, are not required to further notify affected New York residents
- **Still required to notify the New York attorney general, the New York State Department of State Division of Consumer Protection, and the New York State Division of the State Police.**

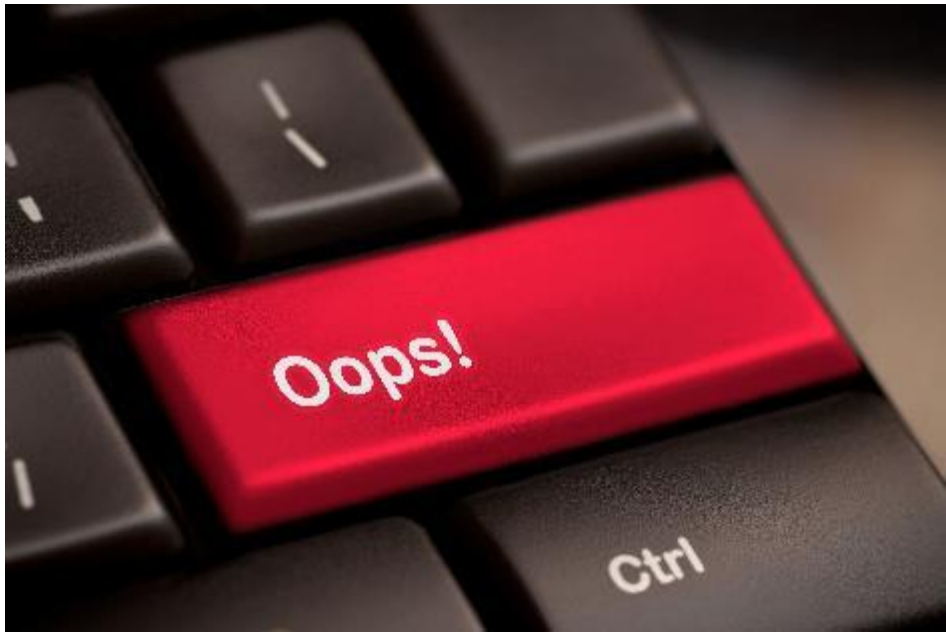
NY SHIELD Act – Other Compliance Laws

- **SHIELD does not apply to any person or business subject to and compliant with the security requirements of GLBA, HIPAA, Part 500, or "any other data security rules and regulations** of, and the statutes administered by, any official department, division, commission or agency of the federal or New York state government … ."
- Section §899-bb is **silent as to how an entity can prove that it is compliant** with any of these regulatory schemes.
- **Because compliance is measured at a point in time, it is possible** under §899-bb for a bank subject to GLBA or a hospital subject to HIPAA **to fall out of compliance with their primary regulator, and therefore become ineligible for the "compliant regulated entity" caveat** built into §899-bb.

New York Law Journal F. Paul Greene, Attorney, Harter-Secrest

NY SHIELD Act – Inadvertent Disclosure Exception

- **"Inadvertent disclosure** by persons authorized to access private information" **if "such exposure will not likely result in misuse of such information, or financial harm** to the affected persons **or emotional harm** in the case of unknown disclosure of online credentials."
- If you take advantage of this you must **document your determination and maintain it for at least five years**.
- **If more than 500 New York residents are affected, you must provide that written determination to the New York Attorney General within 10 days of making it.**



NY SHIELD Act – Reasonable Safeguards

- Businesses must **develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity** of the private information.
- **Businesses in compliance with laws like HIPAA and the GLBA are considered in compliance** with this section of the law.
- Small businesses are subject to the reasonable safeguards requirement, however safeguards may be *"appropriate for the size and complexity of the small business, the nature and scope of the small business's activities, and the sensitivity of the personal information the small business collects from or about consumers."*
- Small business = any business with fewer than fifty employees, less than $3 million in gross annual revenue in each of the last 3 years, or less than $5 million in year-end total assets.

NY SHIELD Act – March 21, 2020 – Administrative, Technical, Physical Security Program

- Risk assessments
- Employee training
- Selecting vendors capable of maintaining appropriate safeguards
- Implementing contractual obligations for those vendors
- Disposal of private information within a reasonable time period

NY SHIELD Act – Penalties

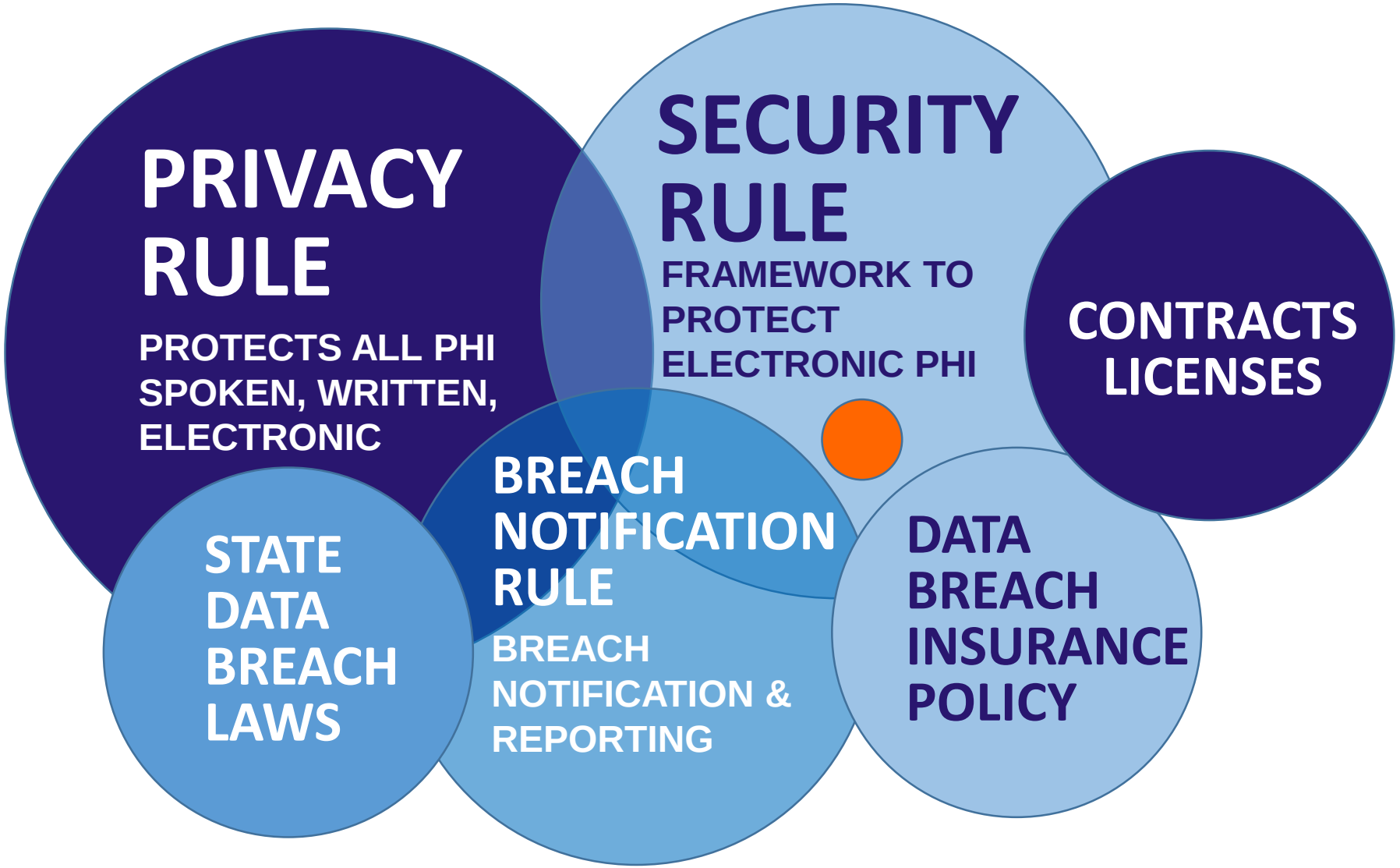
- **No private right of action** (but…)
- Class action litigation is not available.
- **Attorney general may obtain civil penalties.**
- **For data breach notification violations that are *not* reckless or knowing, the court may award damages for actual costs or losses** incurred by a person entitled to notice, **including consequential financial losses.**
- **For knowing and reckless violations, the court may impose penalties of the greater of $5000 dollars or up to $20 per instance with a cap of $250,000.**
- **For reasonable safeguard requirement violations, the court may impose penalties of not more than $5,000 per violation.**

NY SHIELD Act – Basis for Litigation

"…enterprising litigants are certain to refer to (the SHIELD Act's) substantive security requirements as a new floor in New York, at least when alleging negligence in relation to a data breach."

New York Law Journal F. Paul Greene, Attorney, Harter-Secrest

Assess, Correct, & Maintain Total Compliance



Common Issues

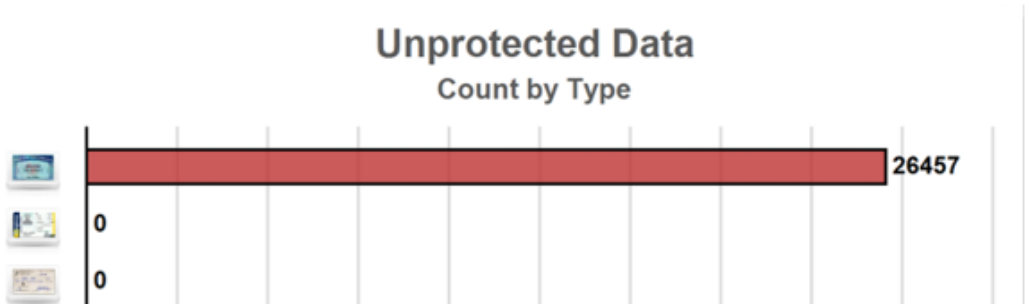
- Unencrypted Protected Health Data
- Unencrypted Workforce Member Data
- Old, unsupported software
- Inconsistent Security Patches
- Inconsistent Anti-virus deployment
- Missing Business Associate Agreements
- Unsecured copiers
- Former workforce members and vendors with continued access

Social Security Numbers on Unencrypted Local PC

3.3 - [redacted]2UA4242HVW

Operating System	IP Address
Windows 7 Professional	172.40.11.37

3.3.1 - Potential Liability



Potential Liability

$5,807,186

Your Next Steps

- **Incident Response Plan Update**
  - Current NY Data Breach Law
  - Other regulations – HIPAA, DFS 500, GLBA, Banking, SEC, FINRA,
  - NEW - SHIELD Act notification and reporting requirements
- **Stay compliant with HIPAA**
  - RECOMMENDATION: Ongoing validation by an independent third-party expert
- **Implement Security Program beyond HIPAA**
  - Don’t just think of customer/client/patient/member data
  - Protect HR, Payroll, Workforce Driver’s info, accident reports, etc.
  - RECOMMENDATION: Ongoing validation by an independent third-party expert

How We Can Help You Protect Your Individuals, Your Brand, and Your $$

- **Compliance Validation/ Gap Analysis**
  - Federal Laws – HIPAA, FERPA
  - State Laws – NYS SHIELD Act
  - Contracts
  - Industry Requirements
  - Cyber Insurance Compliance Review
- **1-year Consulting**
  - For Compliance Officers, IT Directors, and Executives
  - Not just IT
  - Not Just Reports
  - No IT Products or Services

Contact us with questions.

mike@semelconsulting.com

rose@semelconsulting.com

FREE CYBERSECURITY & COMPLIANCE CHECKUP

https://semelhipaa.com/freecpcheckup