Anatomy and Pathology of a Data Breach

March 27, 2012 | Washington, D.C.

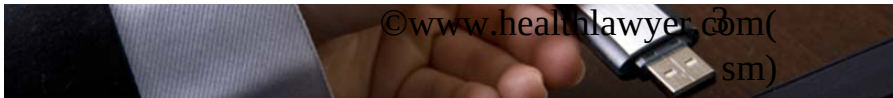
PRESENTERS:
Alan S. Goldberg, Esq., Sharon D. Nelson, Esq. John W. Simek

HIPAA SUMMIT

HIPAA Is About

S t a n d a r d s

Two Elements = Compound



Data Breach Challenges

HIPAA
HITECH

State Laws

Contracts

Be Careful Out There!

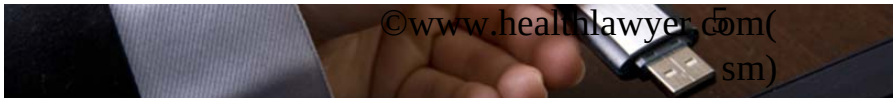
LITIGATION HOLD

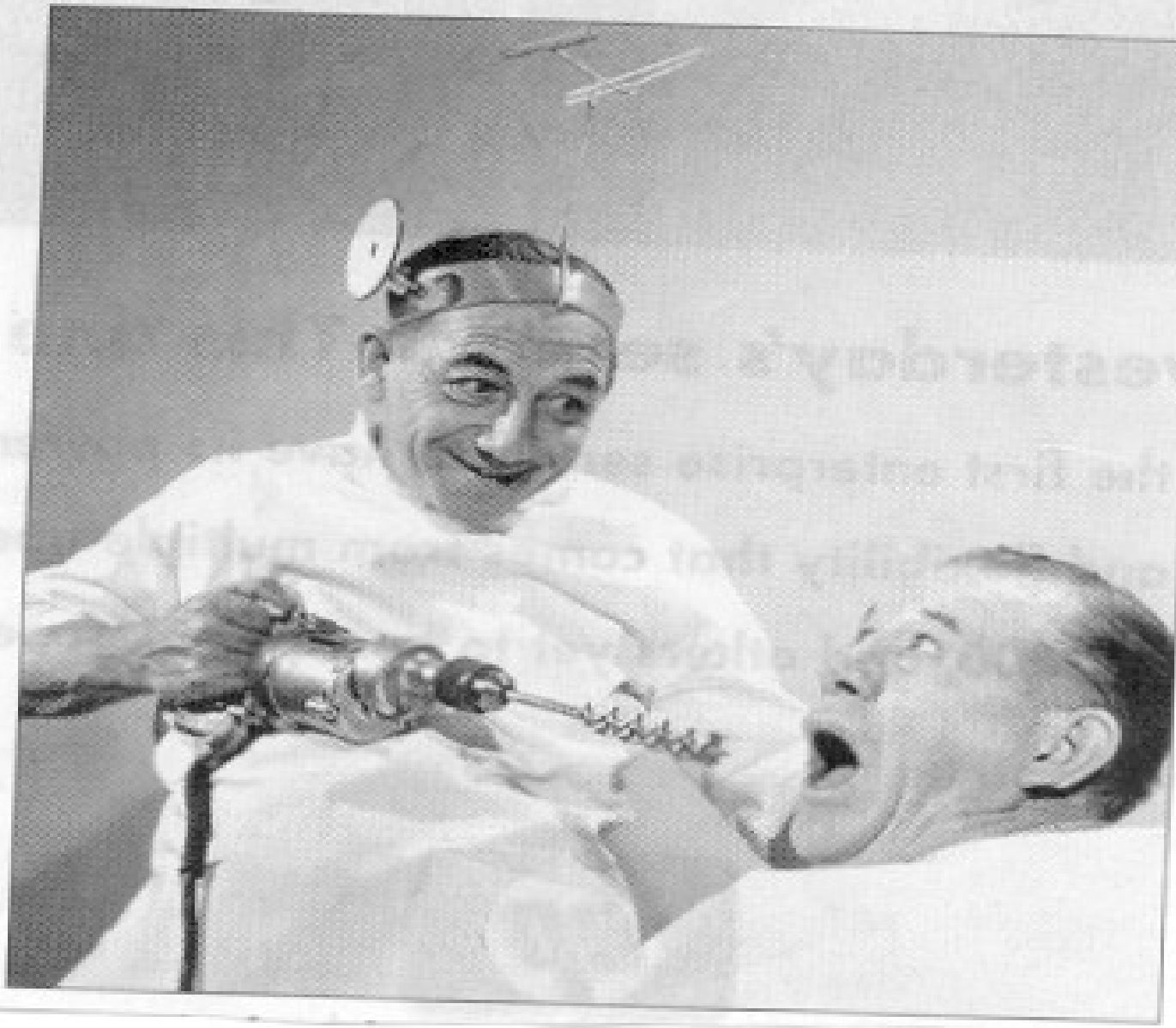
LITIGATION HOLD

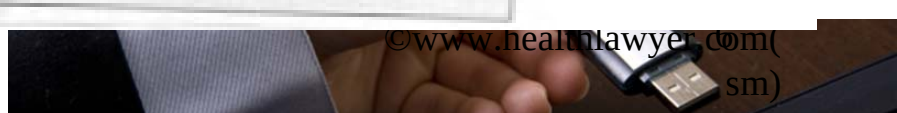
LITIGATION HOLD

LITIGATION HOLD

LITIGATION HOLD







It's All In the Numbers

= >500

<500 LOG

OCR

>500 MEDIA

How Many Individuals Involved?

Legal Challenges

Federal Law

Tort & Contract Law

State Law

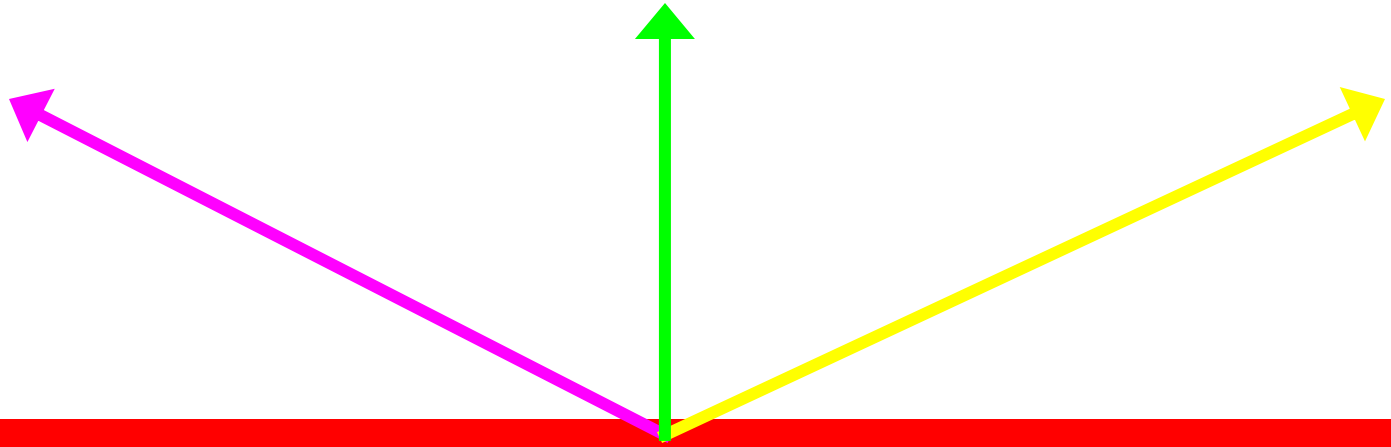
Consequences of Data Breach

Encryption

Not Optional

Security Rule

Addressable



Unsecured Protected Health Information

How Government Prosecutors See Data Breach Abusers

Why is this man smiling?

Practice Safe Computing!

www.healthlawyer.com

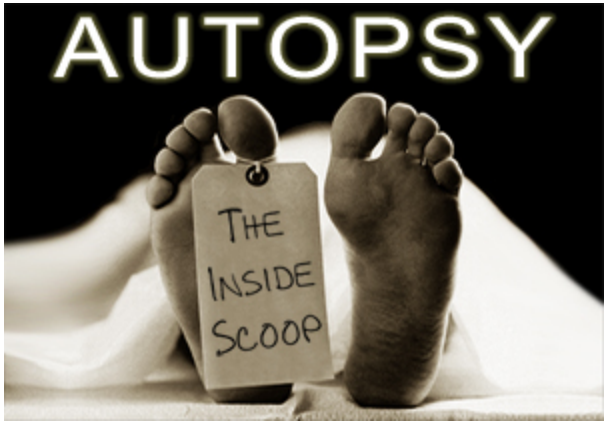
You've been breached – now what?

- Implement your Incident Response Plan
- Call your lawyer
- Get your information security experts in ASAP with your lawyer
- Be forewarned: The first hour with your experts has been called The Upchuck Hour

Don’t assume it is kids – or that it will go away

The First Steps in Investigating a Breach

- It is a little like an autopsy
- You've got a dead body (or a breach) – you must figure out what happened
- What data are they accessing? (a clue to motive)
- What credentials do they have?
- Where are they? (IP addresses)



The First Steps in Investigating a Breach

- Preserve the Logs
- Is it an active breach?
- Identify compromised components
- Identify accessed data
- Origination of attack
- Is there continued risk?
- Forensic preservation

Containing the Breach

- Do you want the breach to continue during the investigation? You might.
- How did they get in?
- Closing the point of entry doesn't help once they are in

Comply with data breach notification laws

Remediation of the problem(s) that caused the breach

- Patch
- Updates
- Access controls
- Data restoration
- Possible equipment replacement
- Additional logging and alerts

Full blown security assessment post-breach

- Penetration testing
- Policy & procedure review
- Vulnerability assessment
- Inventory
- Access controls
- Physical security

An ounce of prevention is better than a pound of cure

- FAR cheaper than a breach
- Get an independent third party audit (both of your network(s) and policies)
- Should be done at least annually, perhaps twice a year
- Policies should be reviewed annually

Security assessments – never by your IT department or IT provider

Number of Systems	Flat Fee Cost
Up to 4 Devices	$2,000.00
5 to 25 Devices	$3,500.00
26 to 50 Devices	$7,000.00
51 to 75 Devices	$10,500.00
76 to 100 Devices	$14,000.00
Over 100 Devices	Call For Pricing

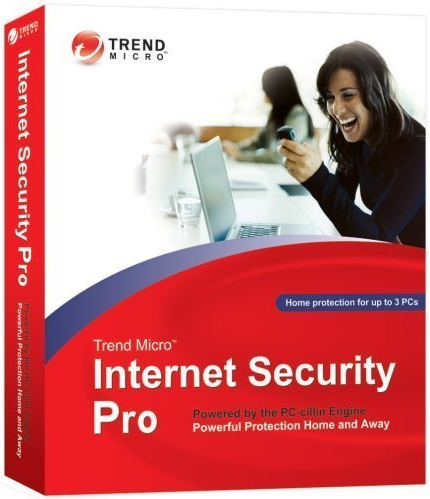
How breaches have happened and lessons learned

Two recent attempted hacks into Sensei

- Hundreds of brute force attacks in short span of time
- One from colo in Reston
- One from China
- Operated as a denial of service attack, bogging the network down
- Blocked those IP addresses
- Attempted to exploit default IDs – and in one attack, it was targeted – they knew our names

Small business office

- Did not have up-to-date enterprise security suite
- Breach had been operative for months
- Owner relied on outside IT consultants
- Important to ask questions and to have security audits
- IT consultant are NOT security experts!



Hack of EPA

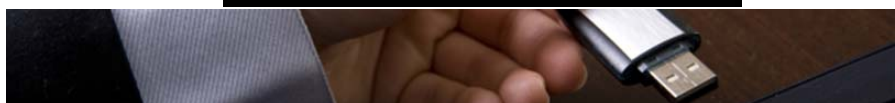
- By fired employee
- Destroyed a lot of files, changed passwords, etc.
- They forgot to kill his remote access

Elliott Greenleaf & Siedzikowski

- PA firm suing William Balaban and his new firm, Stevens & Lee.
- Alleged to have taken 78,000 files
- Used Dropbox to sync the files
- First known case of Dropbox as vehicle for breach

Puckett and Faraj- 2012

- Website hacked by Anonymous
- 3 GB of e-mail taken and released
- Defended Marine guilty of killing 24 Iraqis
- E-mails included details from sexual assault victims
- Also, e-mail of former partner (defended Guantanamo detainees)
- E-mail hosted by website provider
- Another possible vulnerability



Law firm espionage

- West Virginia attorney figured out how another firms attorneys accessed their e-mail (first initial, last name)
- Began spying on wife
- Moved to all the partners
- Make complex passwords

Nemours - 2011

- 3 unencrypted backup tapes disappeared along with the locked cabinet they were stored in
- Will now move toward encryption and offsite secure storage of non-essential backup media
- 1.6 million affected
- Fourth largest data breach
- Encryption, encryption, encryption

TRICARE breach

- 4.9 million military patients affected - largest reported since the **HIPAA breach notification rule,** mandated under the **HITECH Act,** took effect in September 2009
- Backup tapes stolen on Sep. 13th from car of a business associate, Science Applications International Corp.
- Some data encrypted, some not
- Radio and GPS also stolen
- Encryption, encryption, encryption

Stanford Hospital and Clinics

- Oct. 10 2011 press report
  - Nearly 20,000 patients affected
  - Data given to subcontractor
  - Subcontractor decrypted data
  - Gave to job applicant to make bar graphs
  - She didn't know it was real and posted it online (studentoffortune.com) seeking help
- Lessons
  - Share data only when needed – access control
  - Scrutinize partners' security policies and practices

Questions?