

HIPAA, Data Breaches, Identity Theft: What You Don't Know Can Hurt You

The Kentucky Meeting
Kentucky Dental Association

Presented by:

Pat Little, DDS, FAGD, CFE

**HIPAA Compliance, Data Breaches and Identity Theft:
What You Don't Know Can Hurt You!**

**The Kentucky Meeting
Kentucky Dental Association**

Presented by:
Pat Little, DDS, FAGD, CFE

Disclosure

Prosperident

- Senior Fraud Examiner
- Independent contractor

Legacy Transitions

- Dental Transitions Consultant
- Independent contractor

HIPAA Overview

Final Rule

- September 23, 2013

Privacy Rule

Security Rule

Breach Notification Rule



HIPAA Enforcement

Civil

- \$100 - \$50,000 per violation
- \$1,500,000 (maximum)

Criminal

- \$50,000 & 1 year (misuse)
- \$100,000 & 5 years (reckless disregard)
- \$250,000 & 10 years (sale or transfer)



The Privacy Rule

Privacy/Security Officer

Notice of Privacy Practices

Forms, patient requests, logs



The Security Rule

Applies to ePHI

Both at rest and transmission

Security Risk Assessment



The Breach Notification Rule

Notification not required if:

- Data appropriately secured
- Example: encryption

Breach <500

- Maintain log
- Report annually to HHS

Breach >500

- Notify HHS immediately
- Notify Media

Risk Assessment Analysis

Implementation standards

- Administrative
- Physical
- Technical

Required vs Addressable

Addressable ≠ Optional

Identity Theft: Two Basic Methods

Low-tech

High-tech

Types of Identity Theft

New account

Account takeover

Criminal

Types of Identity Theft

Business

Identity cloning

Medical - Dental

Medical – Dental Identify Theft

Fastest growing

48% of patients would switch providers

Black market: \$50 vs \$1

source: FBI Bulletin

706.263.4450
pat@patlittle.com

www.patlittle.com
www.legacypracticetransitions.com

Medical – Dental Identify Theft

HIPAA implications

State board involvement

Financial consequences



Manhattan Dental Office Breach

District Attorney Cyrus Vance's office announced today that it had indicted five people for allegedly belonging to an identity theft ring that stole the identities of patients at a Manhattan dental office.

www.consumeraffairs.com

Manhattan Dental Office Breach

"their personal information made it into the hands of thieves, yet there was nothing those customers could've done to prevent it. A chain is only as strong as its weakest link, and your personal information is only as secure as the least-secure company that has it."

District Attorney Cyrus Vance
February 5, 2015

FTC Warning to Patients

Statement for services not rendered

Unfamiliar EOB

Collection calls



FTC Warning to Patients

Adverse record on credit report from health provider

Plan limit reached

Insurance denial



Patient Rights HIPAA

Obtain copies of records

Report mistakes
Request corrections

Accounting of Disclosures

Who received my information?
What information was sent?
When was it sent?
Why was it sent?



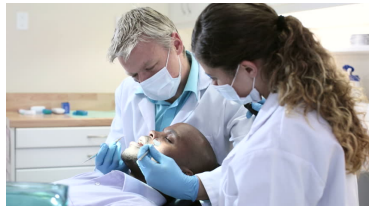
Provider Responsibilities

HIPAA compliance

Full-team training

IT partnership

Vigilance



Provider Responsibilities

Identify your patients

Mr. & Ms. Smiles

The Sisters



Fax Precautions - ADA

Confirm number –call first

Private location

Prohibit redial

“Confidential” cover sheet



Social Media Precautions

HIPAA violations

Use care when responding

Watch SLAPP suits

Strategic Lawsuits against public participation

Social Media Policy



Identity Theft: Low-Tech

Medical, dental records found in church recycling dumpster



Low-Tech: Sara Needleman

“The people I would hire were meth addicts, and the dumber the better.”

“I looked for people strung out the most – people who would steal from their own mother!”



AARP Bulletin: September 2006

Sara Needleman's Methods

Dumpster diving

Mail-boxing

Department store temps

Medical – Dental temps



Other Low-Tech Methods

Telephone scams

Job related

Home related
Friends and babysitters

Shoulder surfing



Identity Theft – High Tech

Hacking

Phishing

Spyware/Adware

Viruses & Trojans



Identity Theft: Hacking

Hacked HVAC vendor

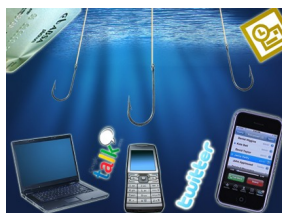
Used vendor as bridge

Planted malware at point
of sale locations



Identity Theft: Phishing

The act of acquiring information
by appearing to be a trustworthy
source in an electronic
communication.



Account Balance: \$0
Your BANK TRANSFER DEACTIVATED (CALL YOUR BANK NOW)
To: pat@prosperident.com

© 2016 - Skril

Dear pat@prosperident.com,

Your account has just been credited with USD 12,780.60 by Snap Cash Payments LTD.

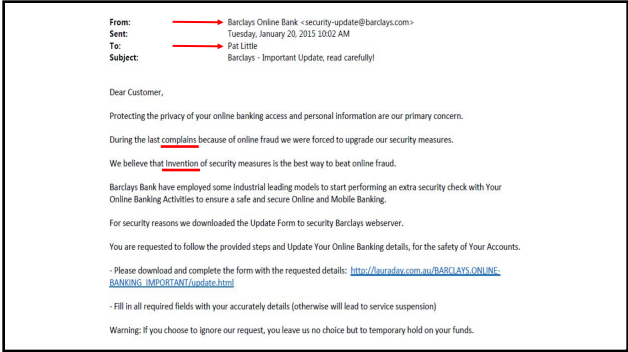
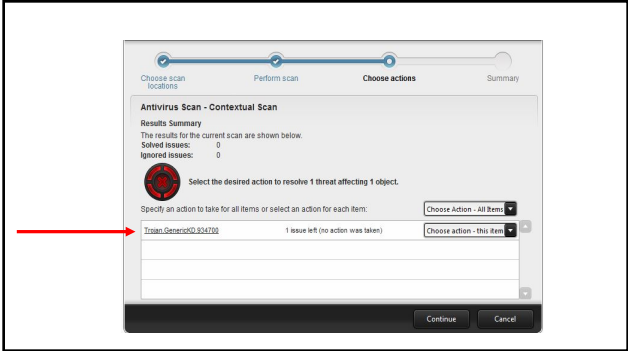
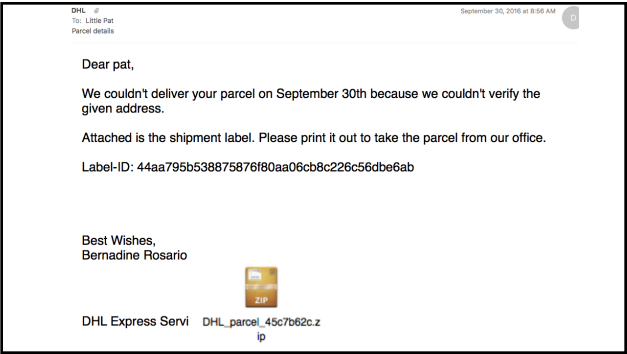
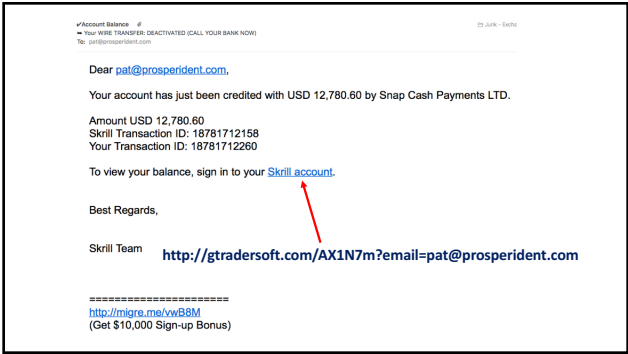
Amount USD 12,780.60
Skrill Transaction ID: 18781712158
Your Transaction ID: 18781712260

To view your balance, sign in to your [Skrill account](#).

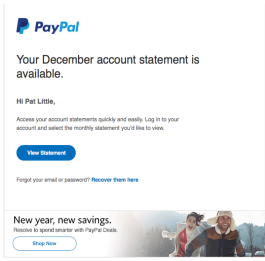
Best Regards,

Skrill Team

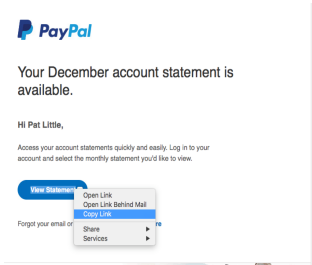
=====
<http://migre.me/xwB8M>
(Get \$10,000 Sign-up Bonus)



Legitimate or Sinister?



How Can You Check?

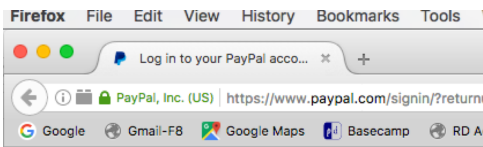


Hypertext Transfer Protocol Secure

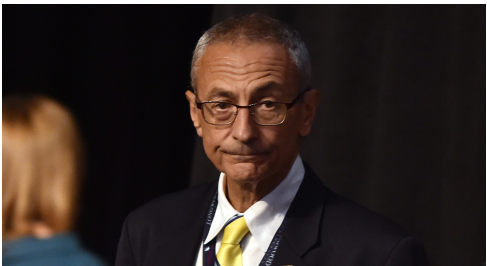
↓

<https://epl.paypal-communication.com/T/v.....>

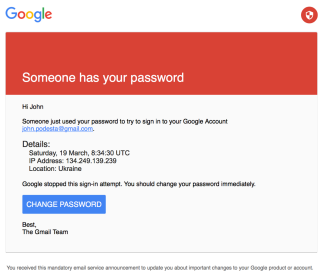
What You Should See

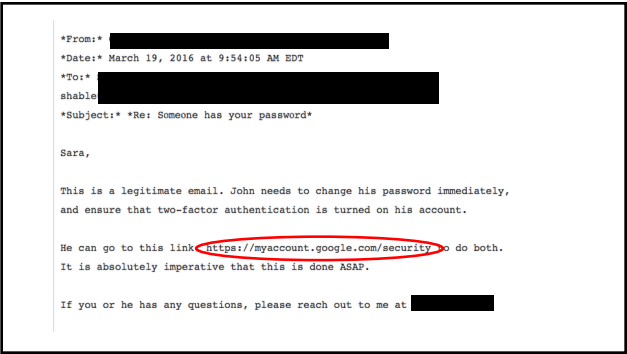
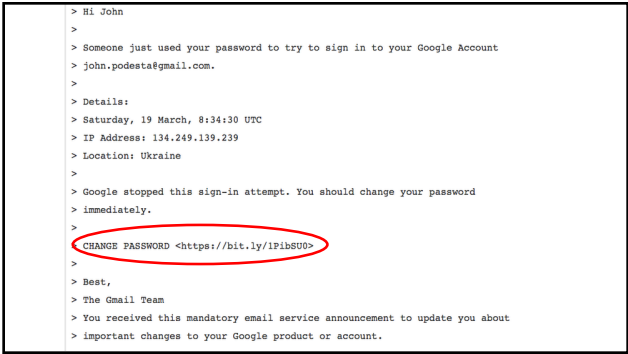


Who Is This? Why Is He not Smiling?



The Infamous Email






No Phishing

Don't take the bait!

Caution opening attachments

Look for https://


Access through web-site

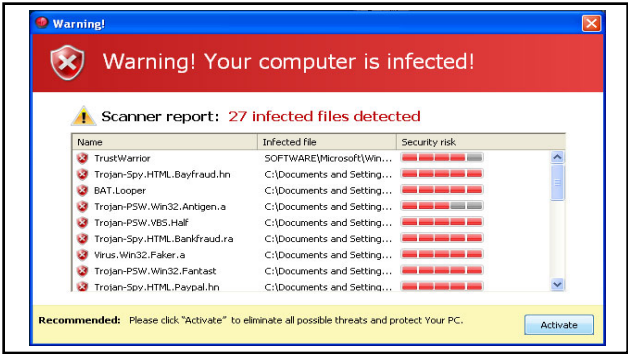


Don't get hooked by an email scam.

Scareware

A type of malware designed to trick victims into purchasing useless and potentially dangerous software.






Ransomware

Similar to Scareware but more insidious

Holds computer hostage (encryption) until a ransom is paid





What Happened?

Resorted to paper and faxing

Paid \$17,000 ransom

Where were the backups?

Where was the disaster recovery plan?

Columbia Presbyterian Medical Center

Additional Security Measures

Secure passwords

Proper security questions

Log-off

Short interval screen savers

High Tech or Low Tech?

David Kernell

2016 Most Popular Passwords (3.3 million)

1. 123456

2. password

3. 12345

4. 12345678

5. football

6. qwerty

7. 1234567890

8. 1234567

9. princess

10. 1234

11. login

12. welcome

13. solo

14. abc123

15. admin

16. 1212

17. flower

18. password

19. dragon

20. sunshine

21. master

22. hottie (new)

23. loveme (new)

24. zaq1zaq1

25. password1

Splashdata.com

Which Password Is More Secure?

A: PrXyc.N(n4k77#L!eVdAfp9

B: D0g.....

https://www.grc.com/haystack.htm

1 Uppercase2 Lowercase4 Digits1 Symbol8 Characters

Agp-9481

Enter and edit your test password in the field above while viewing the analysis below.

Brute Force Search Space Analysis:

Search Space Depth (Alphabet):	26+26+10+33 = 95
Search Space Length (Characters):	8 characters
Exact Search Space Size (Count): <small>(count of all possible passwords with this alphabet size and up to this password's length)</small>	6,704,780,954,517,120
Search Space Size (as a power of 10):	6.70 x 10 ¹⁵

Time Required to Exhaustively Search this Password's Space:

Online Attack Scenario: <small>(Assuming one thousand guesses per second)</small>	2.13 thousand centuries
Offline Fast Attack Scenario: <small>(Assuming one hundred billion guesses per second)</small>	18.62 hours
Massive Cracking Array Scenario: <small>(Assuming one hundred trillion guesses per second)</small>	1.12 minutes

Note that typical attacks will be online password guessing limited to, at most, a few hundred guesses per second.

Password Manager Tools

Keychain (Apple)

1Password

Msecure

LastPass

Biometric may ultimately augment/replace

Preventing (?) Attacks

Regular backups

External drives

Cloud-based

Firewall

Security Software

IT Professional

Preventing (?) Attacks

Keep software updated

Limit Administrator activity

Use Standard User account

Removing Malware

Security Software

Computer manufacturer

Bootable recovery tool

IT Professional

Additional Security Measures

Privacy settings

Avoid unsecured Wi-Fi

Disable Wi-Fi and Bluetooth unless needed

Additional Security Measures

Activate email and text alerts

Keep software updated
(automatic updates)

Verify privacy settings

Monitor USB ports



Smartphone Security

Use security code

Enable "find my phone" service
Remote lock and/or data deletion

Encryption and password protection apps

Download apps from trusted sources

Virtual private network (VPN)



Contact Information

Pat Little, DDS, FAGD

706.263.4450

pat@patlittle.com

www.patlittle.com

STANDARDS/ IMPLEMENTATION SPECS	REQUIRED ADDRESSABLE
Administrative Safeguards	
Security Management Process 164.308(a)(1)	
Security Management Process	R
Risk Analysis	R
Risk Management	R
Sanction Policy	R
Information System Activity Review	R
Assigned Security Responsibility 164.308(a)(2)	
Assigned Security Responsibility	R
Workforce Security 164.308(a)(3)	
Workforce Security	R
Authorization and/or Supervision	A
Workforce Clearance Procedure	A
Termination Procedures	A
Information Access Management 164.308(a)(4)	
Information Access Management	R
Isolating Health care Clearinghouse Function	R
Access Authorization	A
Access Establishment and Modification	A
Security Awareness and Training 164.308(a)(5)	
Security Awareness and Training	R
Security Reminders	A
Protection from Malicious Software	A
Log-in Monitoring	A
Password Management	A
Security Incident Procedures 164.308(a)(6)	
Security Incident Procedure	R
Response and Reporting	R
Contingency Plan 164.308(a)(7)	
Contingency Plan	R
Data Backup Plan	R
Disaster Recovery Plan	R
Emergency Mode Operation Plan	R
Testing and Revision Procedure	A
Applications and Data Criticality Analysis	A
Evaluation 164.308(a)(8)	
Evaluation	R
Business Assoc. Contracts & Other Arrangements 164.308(b)(1)	
Business Associate contracts and other arrangements	R
Written Contract or Other Arrangement	R

STANDARDS/ IMPLEMENTATION SPECS	REQUIRED ADDRESSABLE
Physical Safeguards	
Facility Access Controls 164.310(a)(1)	
Facility Access Controls	R
Contingency Operations	A
Facility Security Plan	A
Access control and validation procedures	A
Maintenance records	A
Workstation Use 164.310(b)	
Workstation Use	R
Workstation Security 164.310(c)	
Workstation Security	R
Device and Media Controls 164.310(d)(1)	
Device and Media Controls	R
Disposal	R
Media Re-use	R
Accountability	A
Data backup and storage	A
Technical Safeguards	
Access Control 164.312(a)(1)	
Access Control	R
Unique User Identification	R
Emergency Access Procedure	R
Automatic Logoff	A
Encryption and Decryption	A
Audit Controls 164.312(b)	
Audit Controls	R
Integrity 164.312(c)(1)	
Integrity	R
Mechanism to Authenticate Electronic Protected Health Information	A
Person or Entity Authentication 164.312(d)	
Person or Entity Authentication	R
Transmission Security 164.312(e)(1)	
Transmission Security	R
Integrity Controls	A
Encryption	A