

2014–2015 Healthcare Breaches – Is History Repeating Itself ?

Todd Fitzgerald, Global Director
Information Security, Grant Thornton
International, Ltd.

Today's Webinar is Sponsored by:



GODFREY KAHN S.C.



Date Recorded:
April 6, 2015

HIPAA COW Mission



- ▶ Assist HIPAA Covered Entities, Business Associates, and other interested parties in implementing HIPAA's Privacy, Security and EDI Standard Transaction provisions, as amended over time.
- ▶ Foster public education about HIPAA.
- ▶ Facilitate and streamline HIPAA implementation through identification of best practices.
- ▶ Reduce duplicate efforts among entities obligated to comply with HIPAA.
- ▶ Offer opportunities for partnering and collaborating between entities implementing HIPAA.
- ▶ Identify and evaluate new or difficult HIPAA interpretation issues.

Disclaimer

This document is Copyright © by the HIPAA Collaborative of Wisconsin (“HIPAA COW”). It may be freely redistributed in its entirety provided that this copyright notice is not removed. When information from this document is used, HIPAA COW shall be referenced as a resource. It may not be sold for profit or used in commercial documents without the written permission of the copyright holder. This document is provided “as is” without any express or implied warranty. This document is for educational purposes only and does not constitute legal advice. If you require legal advice, you should consult with an attorney. HIPAA COW has not yet addressed all state pre-emption issues related to this document. Therefore, this document may need to be modified in order to comply with Wisconsin law.



LEGAL NOTICE: HIPAA Collaborative of Wisconsin Content and Liability Disclaimer

The HIPAA Collaborative of Wisconsin (HIPAA COW) shall not be responsible for any errors or omissions contained in materials provided by HIPAA COW. All information is provided on an "AS IS" basis.

HIPAA COW MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED (INCLUDING ANY WARRANTIES OF TITLE, NON-INFRINGEMENT AND IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE) REGARDING ANY INFORMATION CONTAINED IN ITS MATERIALS. THE USER OF THE MATERIALS SHALL ASSUME TOTAL RESPONSIBILITY AND RISK FOR THE USE OF THE MATERIALS. IN NO EVENT SHALL HIPAA COW BE LIABLE FOR ANY DAMAGES WHATSOEVER, INCLUDING BUT NOT LIMITED TO SPECIAL, DIRECT, INDIRECT, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, OR DAMAGES FOR LOST PROFITS, LOSS OF REVENUE, OR LOSS OF USE, ARISING OUT OF OR RELATED TO ANY INFORMATION CONTAINED IN THE MATERIALS PROVIDED BY HIPAA COW, WHETHER SUCH DAMAGES ARISE IN CONTRACT, NEGLIGENCE, TORT, UNDER STATUTE, IN EQUITY, AT LAW OR OTHERWISE.

The content of the materials provided by HIPAA COW is designed to provide accurate and authoritative information in regard to the subject matter covered. It is provided with the understanding that HIPAA COW is not engaged in rendering legal or other professional services. If legal advice or other expert assistance is required, the services of a competent professional person should be sought.



Presenter Disclaimer

- Todd Fitzgerald is the Director of Information Security with Grant Thornton International Ltd. The views expressed in this presentation are solely Todd Fitzgerald's personal views and do not necessarily represent the views of Grant Thornton or its clients or its related entities. The information provided with respect to Todd Fitzgerald's affiliation with Grant Thornton is solely for identification purposes and may not and should not be construed to imply endorsement or support by Grant Thornton of the views expressed herein.



"Grant Thornton" refers to the brand under which the Grant Thornton member firms provide assurance, tax and advisory services to their clients and/or refers to one or more member firms, as the context requires. [Member firm name¹] is a member firm of Grant Thornton International Ltd (GTIL). GTIL and the member firms are not a worldwide partnership. GTIL and each member firm is a separate legal entity. Services are delivered by the member firms. GTIL does not provide services to clients. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another's acts or omissions.

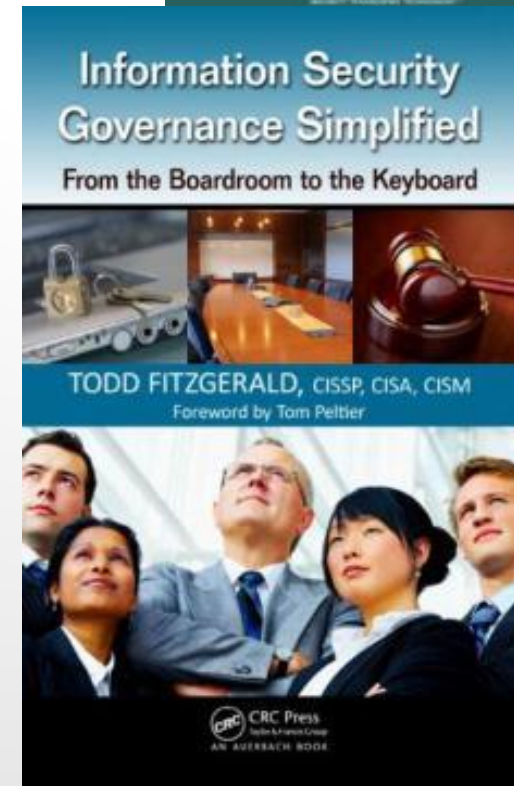
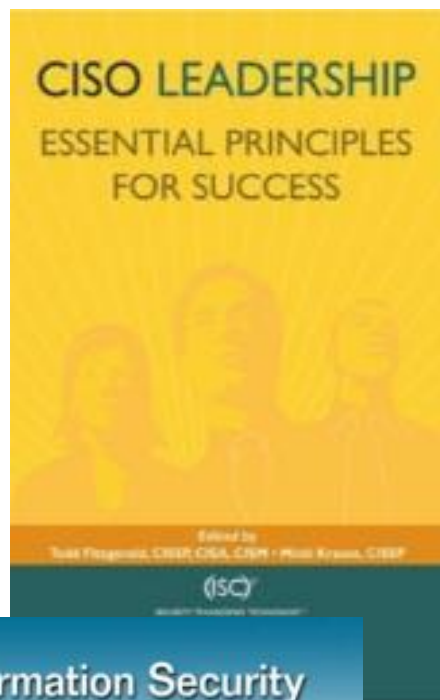
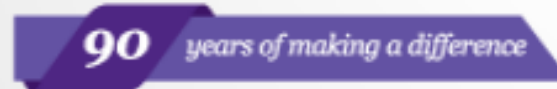
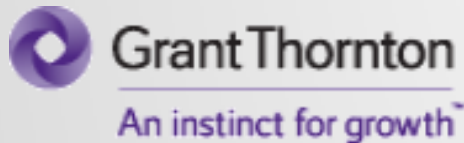


Today's Host



**Todd Fitzgerald, CISSP, CISA,
CISM, CIPP/E, CIPP/US,
PMP, CRISC, ISO27000,
ITILv3f**

Global Director of Information Security
Grant Thornton International Ltd



Today's Agenda

- ▶ Current Breach Trends / Costs
- ▶ Top Healthcare Breaches 2014–2015
- ▶ What Does This Mean For Us Now ?
- ▶ Future Technology Impacting Healthcare



The Current Healthcare/Breach Environment



Trends Impacting Healthcare

Healthcare
Information
Exchanges

More than \$9,210 per capita
spent on Healthcare (2013)

Increased Cyber
insurance

Expanded attack
surface

Medical Identity
Theft (1.8 Million
US Victims)

HIPAA Omnibus
breach and privacy
requirements

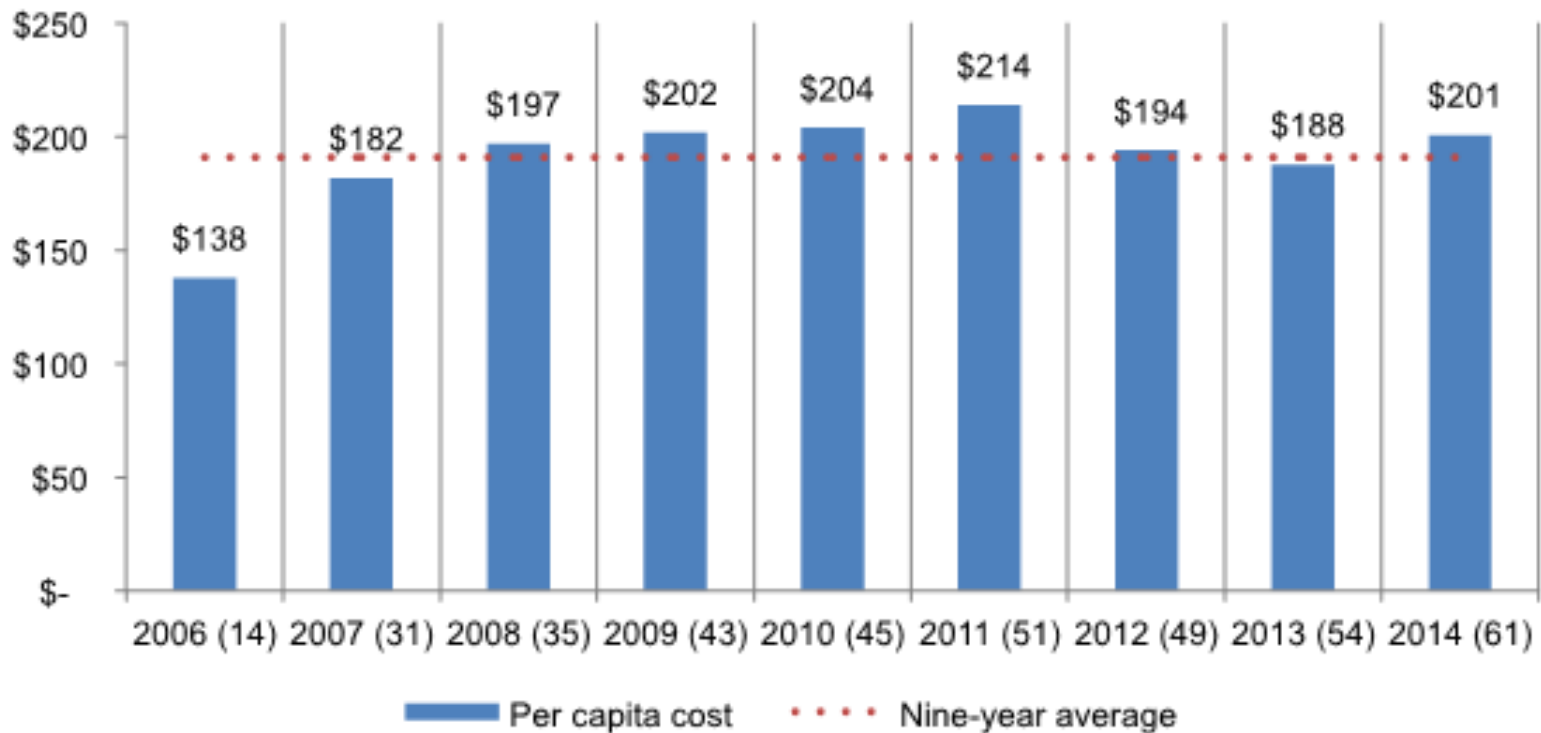
Lack of resources



Source: 2014 Data Breach Industry Forecast - Experian

2014 Cost Per Record is \$201, \$180 With a Strong Security Posture

Figure 1. The average per capita cost of data breach over nine years
Bracketed number defines the benchmark sample size

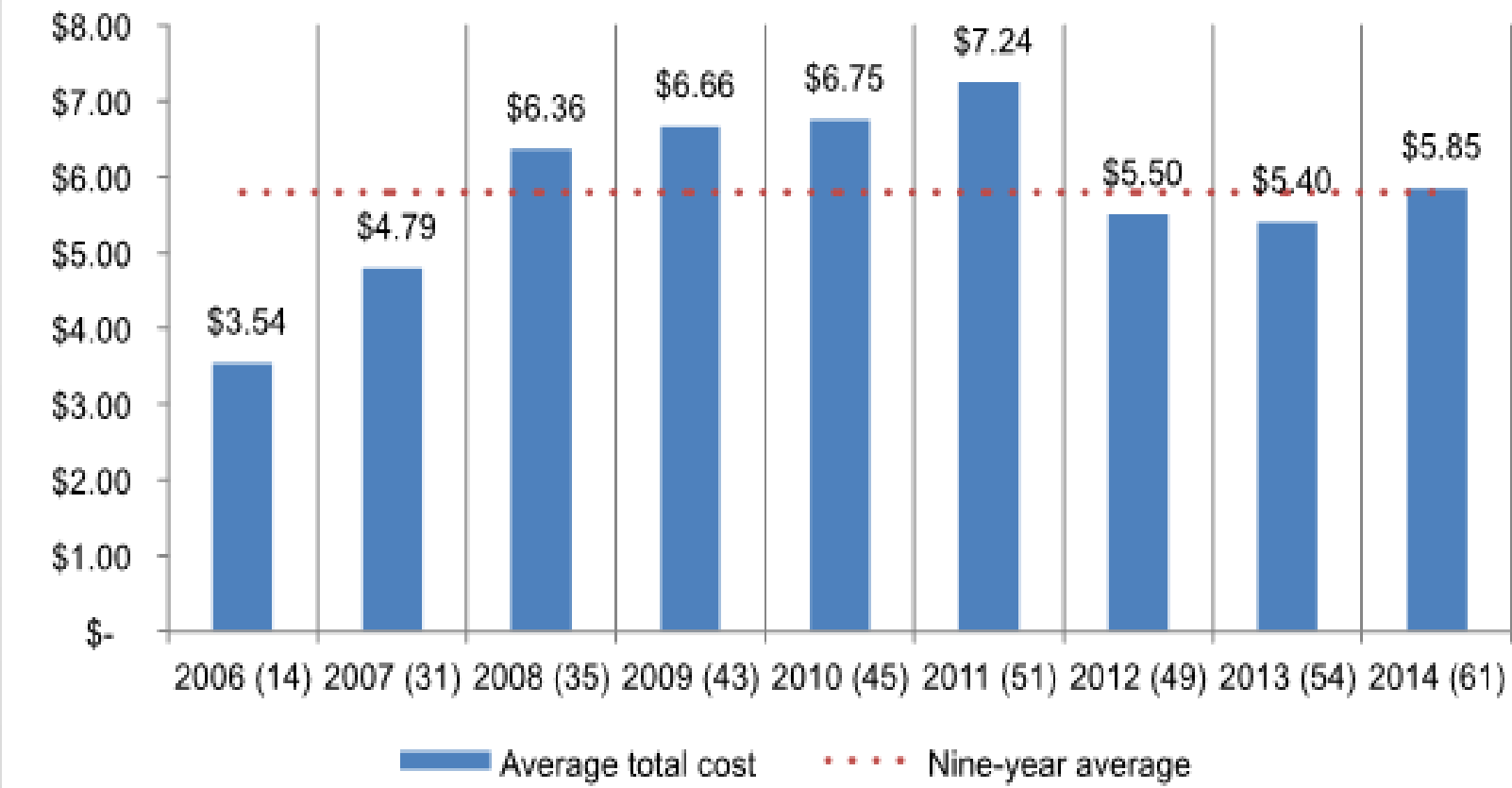


Source: 2014 Ponemon Cost of Data Breach Study US, May, 2014



\$5.85M – 2014 Average Cost per Breach

Figure 2. The average total organizational cost of data breach over nine years
\$000,000 omitted



Source: 2014 Ponemon Cost of Data Breach Study US, May, 2014



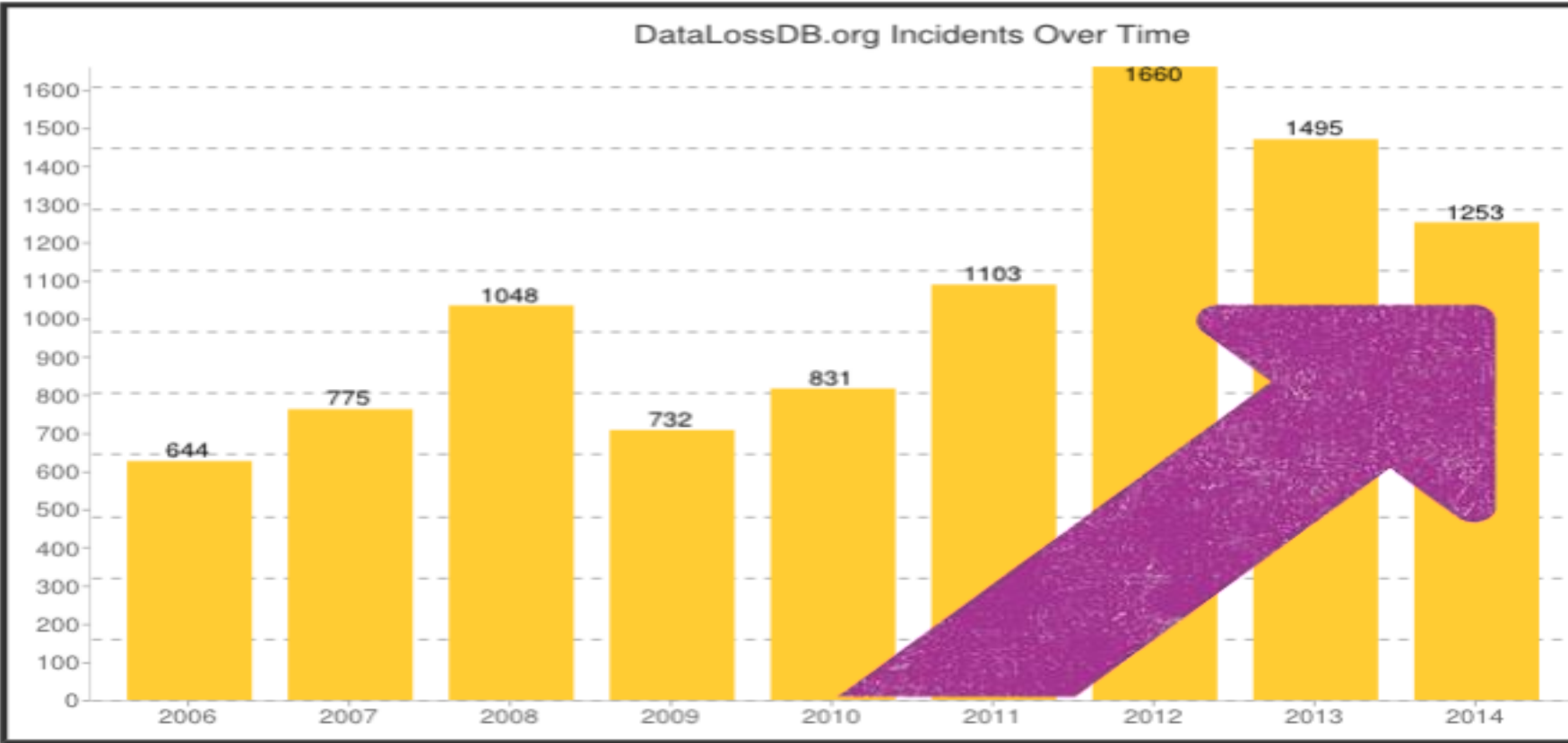
FBI Notified Companies of Breaches



- 3,000 companies notified
- 1,000 agents in FBI
Cybersecurity
- 2/3 of breaches from Russia
& China

Source: Washington Post, 3/24/14

2005-15 Number of Reported Data Breaches Are Increasing



www.datalossdb.org





2014 Data Breach Category Summary

How is this report produced? What are the rules? See last page of report for details. Report Date: 1/5/2015

Page 1 of 1

Totals for Category: Banking/Credit/Financial	# of Breaches: 43	# of Records: 1,198,492
	% of Breaches: 5.5%	%of Records: 1.4%

Totals for Category: Business	# of Breaches: 258	# of Records: 68,237,914
	% of Breaches: 33.0	%of Records: 79.7%

Totals for Category: Educational	# of Breaches: 57	# of Records: 1,247,812
	% of Breaches: 7.3%	%of Records: 1.5%

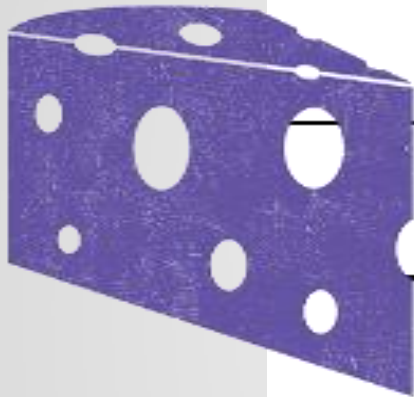
Totals for Category: Government/Military	# of Breaches: 92	# of Records: 6,649,319
	% of Breaches: 11.7	%of Records: 7.8%

Totals for Category: Medical/Healthcare	# of Breaches: 333	# of Records: 8,277,991
	% of Breaches: 42.5	%of Records: 9.7%

Totals for All Categories:	# of Breaches: 783	# of Records: 85,611,528
	% of Breaches: 100.0	%of Records: 100.0%

2014 Breaches Identified by the ITRC as of:	1/5/2015
--	-----------------

Total Breaches:	783
Records Exposed:	85,611,528



**Record
High 783
Breaches
(27.5%
over
2013)**





2014 Data Breach Category Summary

How is this report produced? What are the rules? See last page of report for details. Report Date: 1/5/2015

Page 1 of 1

Totals for Category: Banking/Credit/Financial	# of Breaches: 43	# of Records: 1,198,492
	% of Breaches: 5.5%	%of Records: 1.4%

Totals for Category: Business	# of Breaches: 258	# of Records: 68,237,914
	% of Breaches: 33.0	%of Records: 79.7%

Totals for Category: Educational	# of Breaches: 57	# of Records: 1,247,812
	% of Breaches: 7.3%	%of Records: 1.5%

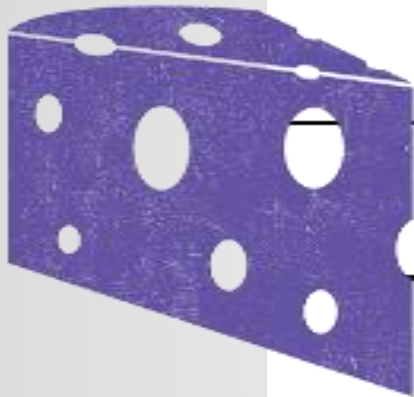
Totals for Category: Government/Military	# of Breaches: 92	# of Records: 6,649,319
	% of Breaches: 11.7	%of Records: 7.8%

Totals for Category: Medical/Healthcare	# of Breaches: 333	# of Records: 8,277,991
	% of Breaches: 42.5	%of Records: 9.7%

Totals for All Categories:	# of Breaches: 783	# of Records: 85,611,528
	% of Breaches: 100.0	%of Records: 100.0%

2014 Breaches Identified by the ITRC as of:	1/5/2015
--	-----------------

Total Breaches:	783
Records Exposed:	85,611,528



Healthcare
42.5% of
the
breaches
reported



Recent Healthcare Breaches



Advocate Healthcare – Previously 2nd largest Healthcare Breach (OCT 2013)

- ▶ Four **unencrypted** computers containing 4 Million Patients stolen July 15, 2013
- ▶ Addresses, DOB, Names and SSNs on PCs
- ▶ Health Insurance data, medical diagnosis and record numbers
- ▶ Breach also reported in 2009 on 812 patients for unencrypted laptop.



2014– Largest HIPAA Settlement To Date Reached

FOR IMMEDIATE RELEASE

May 7, 2014 Contact: HHS Press Office

(202) 690-6343

Data breach results in \$4.8 million HIPAA settlements

Two health care organizations have agreed to settle charges that they potentially violated the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules by failing to secure thousands of patients' electronic protected health information (ePHI) held on their network. The monetary payments of \$4,800,000 include the largest HIPAA settlement to date.

The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) initiated its investigation of New York and Presbyterian Hospital (NYP) and Columbia University (CU) following their submission of a joint breach report, dated September 27, 2010, **regarding the disclosure of the ePHI of 6,800 individuals**, including patient status, vital signs, medications, and laboratory results.



Sutherland Health Systems Breach (3RD Part Billing Vendor–Feb 2014)



**NO ENCRYPTION
(COST < \$400)**



**\$6.8M HIPAA Fine
For Triple-S,
Improper Handling
14,000 Patient
Records**

- Feb, 2014

342,197 MEDICAL RECORDS



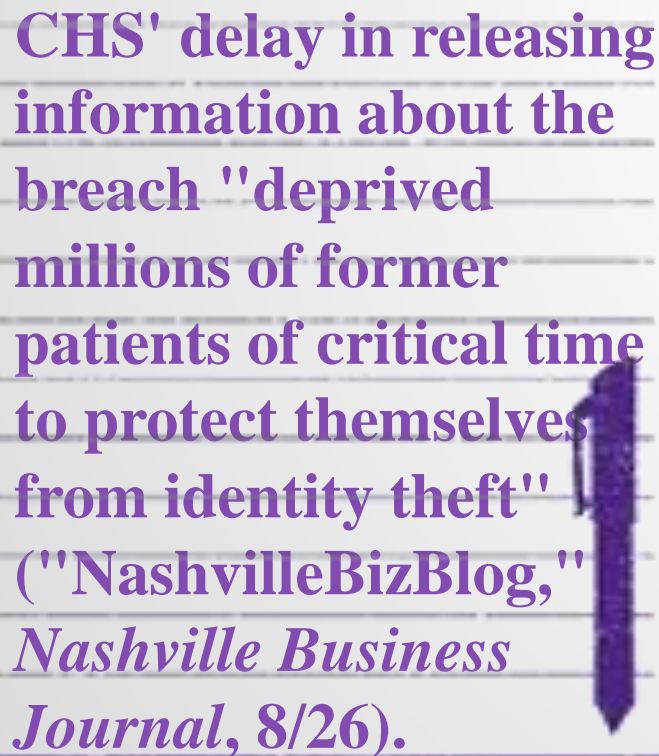
Montana Dept of Health and Human Services Breach (May, 2014)

- Server Hacked containing 1.3 Million Individuals
- Names, Addresses, DOB, SSN
- **Health Assessments, Diagnoses, treatment, health condition, prescriptions, insurance, bank account numbers.**

"This Incident should not impact DPHHS services as none of the information contained on the server was lost and we have a complete back-up of the information



Community Health System Breach (Reported Aug 2014, occurred Apr–Jun)



CHS' delay in releasing information about the breach "deprived millions of former patients of critical time to protect themselves from identity theft" ("NashvilleBizBlog," *Nashville Business Journal*, 8/26).

- Largest hospital system with 206 hospitals in 29 states
- 4.5M Patients
- Heartbleed OPENSLL
- APT? Chinese Hackers early attribution
- Have Cyber insurance, believe impact non-material
- \$75-\$150M (Forbes)

Beyond these, in 2014 there were also 333 Breaches involving 8.2M records

May, 2014– Touchstone Imaging – Folder containing 307,528 patients accessible to Internet

June, 2014 Aventura Hospital and Medical Center, 82,601 people, 3rd data breach in 2 years, Business Associate involved.

July, 2014– ENT Partners of Texas, 789 records, Burglars broke into an office and stole 2 laptops – password protected, not encrypted

July, 2014– Care All Management, Inc., 28,300 records – Improper Disposal



2014 Healthcare Context- Breaches Involving Credit Cards

- Home Depot, 56M+ 53M email addresses
- Neimen Marcus 350K Records, JP Morgan Chase 1 M
- **Sutherland Healthcare Solutions- 338,700 Californians**
- P.F. Chang's - 33 Restaurants, 16 states
- Michaels - 3M Credit Cards
- Goodwill, 868,000 records
- University of Maryland - 309,000 student records
- Paytime, Inc. - 200,000 people
- **State of Montana Dept. of Public Health- 1.3M people**
- VFW- 55,000 people
- Deltek- 80,000 Federal contractors
- Spec's Wine and Spirits - 550,000 Credit Cards



Top 10 2014 HIPAA Breaches

No	Company	Records	Cause
1	Community Health Systems	4.5M	Chinese Hacking (Heartbleed Vulnerability)
2	Xerox State Healthcare, LLC.	2M	Terminated Medicaid Contract, removed patient records from hard drives and servers, allowed others to see (pending legal dispute)
3	Sutherland Healthcare Solutions, Inc	342,197	8 computers stolen (unencrypted)
4	Touchstone Medical Imaging	307,528	Folder exposed to Internet for months
5	Indian Health Service	214,000	Accessed by a Physician employed by a staffing company under contract with HIS.
6	Walgreen Co	160,000	Paper records disclosed
7	NRAD Medical Associates, P.C.	97,000	Previously employed associate accessed billing group system without authorization
8	Visonworks, Inc.	74,944	Replaced a database server, server then disappeared with unencrypted records. Lost a 2 nd server 2 weeks later (another 48,000 records)
9	St. Vincent Hospital and Health Care Center, Inc.	63,325	63,000 letters sent to the wrong patients
10	Onsite Health Diagnostics	60,582	Hacker access

Source: www.datapipe.com/blog/2015/01/28/top-10-hipaa-data-breaches-of-2014



2015 Starting off with a Bang... 208 breaches, 99M Records, 97.9% (Mar, 2015)

Sacred Heart
Billing Vendor
14,177 Records
(email hacking)

3/2/15 – Georgia Dept.
of Community Health
900K Records

Amedisys Home care
Reported 142 Missing
Encrypted drives on
6,909 individuals

Totals for Category: Medical/Healthcare	# of Breaches: 68	# of Records: 99,335,375
	% of Breaches: 32.7	%of Records: 97.9%

Totals for All Categories:	# of Breaches: 208	# of Records: 101,449,874
	% of Breaches: 100.0	%of Records: 100.0%

2015 Breaches Identified by the ITRC as of: 3/30/2015

Total Breaches: 208
Records Exposed: 101,449,874

3/12/15– Virginia
Dept. of Medical
Assistance Services
697,586 Records

3/18/15– Advantage
Consolidated, LCC
151,626 Records



2015–Anthem Breach (Jan)

Anthem was the target of a very sophisticated external cyber attack. Based on what we know now, there is no evidence that credit card or medical information were targeted or compromised.

80
Million



Sensitive
Records

- **Backdoor**
- **Compromised Logins/Passwords**
- **Remote Database Queries**

- **Anomalous Behavior monitored?**
- **Adequate Password Controls?**

2015–Premera Blue Cross – 11 Million Records (Mar)

Information About the Premera Cyberattack

Premera Blue Cross has been the target of a cyberattack. The security of our members' personal information is a top priority. We're taking proactive steps to address this issue and offering free identity protection services to affected members. Please note that only members who were affected by the cyberattack are eligible for this service. For more information, visit <http://www.premeraupdate.com>. Other sites with similar web addresses may be affected. Premera and contain content not including malware. [Find out more \(http://www.premeraupdate.com\)](http://www.premeraupdate.com).

A Message from Premera President and CEO, Jeff Roe

I recognize the frustration that the news of this cyberattack may cause. The privacy and security of our members' personal information is a top priority.....

2015–Premera Blue Cross – 11 Million Records (Mar)

Information About the

Premera Blue Cross has

cyberattack. The security

is a top priority. We're

issue and offering free

affected. Please note that

<http://www.premeraup>

Other sites with similar

Premera and contain

including malware. Find

<http://www.premeraup>

"May have gained unauthorized access to .."

Member Name

Date of Birth

Email Address

Telephone Number

SSN

Member ID Numbers

Bank Account

Information

Claims Information

Clinical Information

- **Data Dates Back to 2002**
- **Attack Began May 5, 2014**
- **OPM 4/18/14 Audit indicated 10 vulnerabilities to be fixed**
- **5 Class Action Lawsuits Filed**



Learning From History



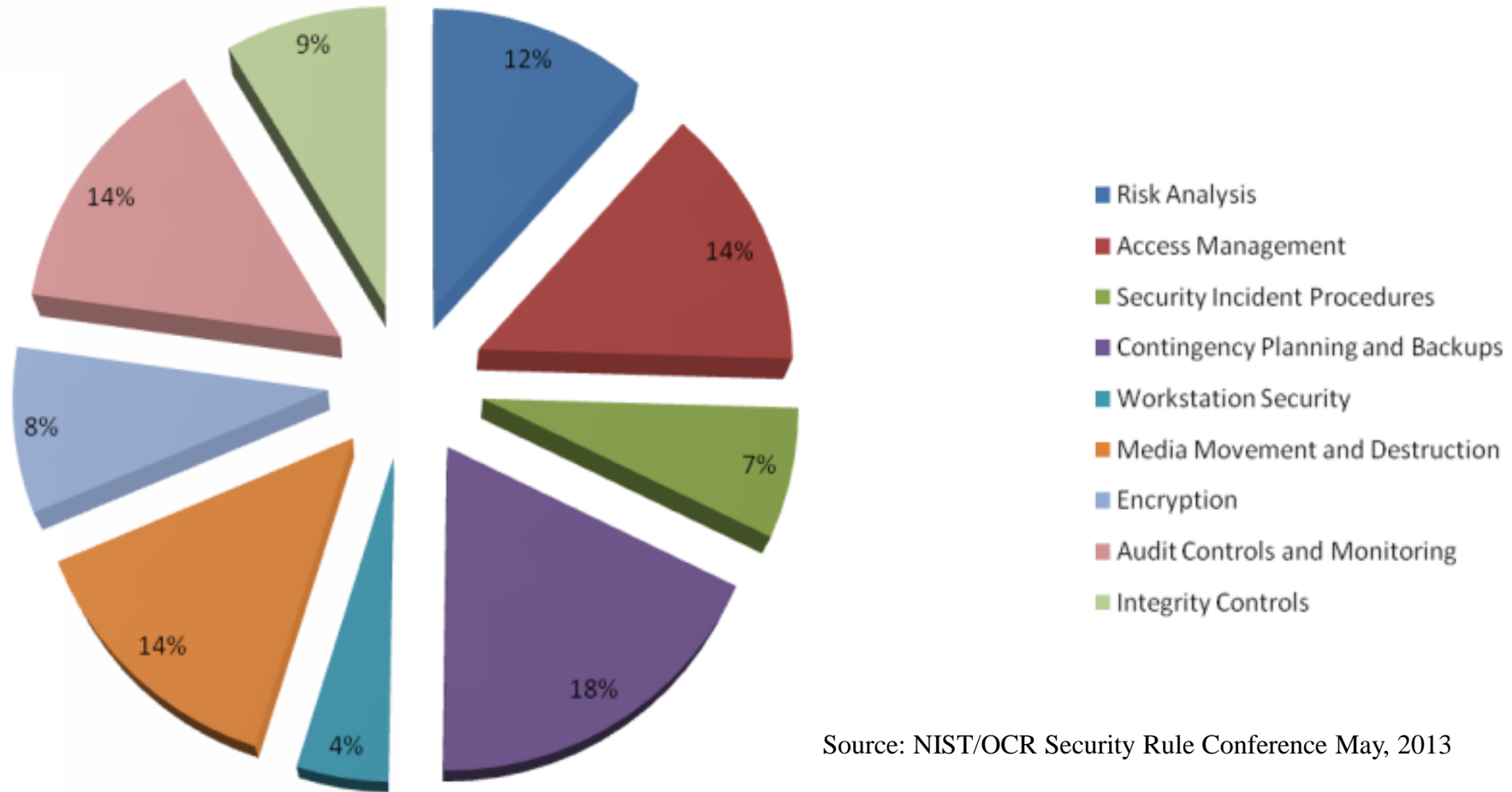
RECALL: 2013 HEALTHCARE DATA BREACHES

Breach	Patients	Cause
Horizon BCBS NJ	840,000	Cable-locked laptop stolen over weekend
Anthem BCBS Indiana	6,000	Software solutions provider
AHIMC Healthcare	729,000	Two password-protected laptops stolen (not encrypted)
Johns Hopkins	9,000	Illegally recorded and saved images of patients with personal equipment
Walgreens	1	\$1.44M awarded-inappropriate pharmacist access
Medical Sol Mgmt.	1,000	Stolen for Medicare Fraud, 12 years in prison
Advocate	4 Million	4 stolen computers
Hope Hospice	800	Sent 2 unsecured emails
IRS	10 Million	15 IRS agents took records, 4 th amendment violation claimed
River Falls	2,400	2,400 Recs-cleaning crew from shredding bin

Source: HeathIT Security, Dec 23, 2013



RECALL: 2012 OCR Audit of 115 Hospitals, Providers, and Clearinghouses ?

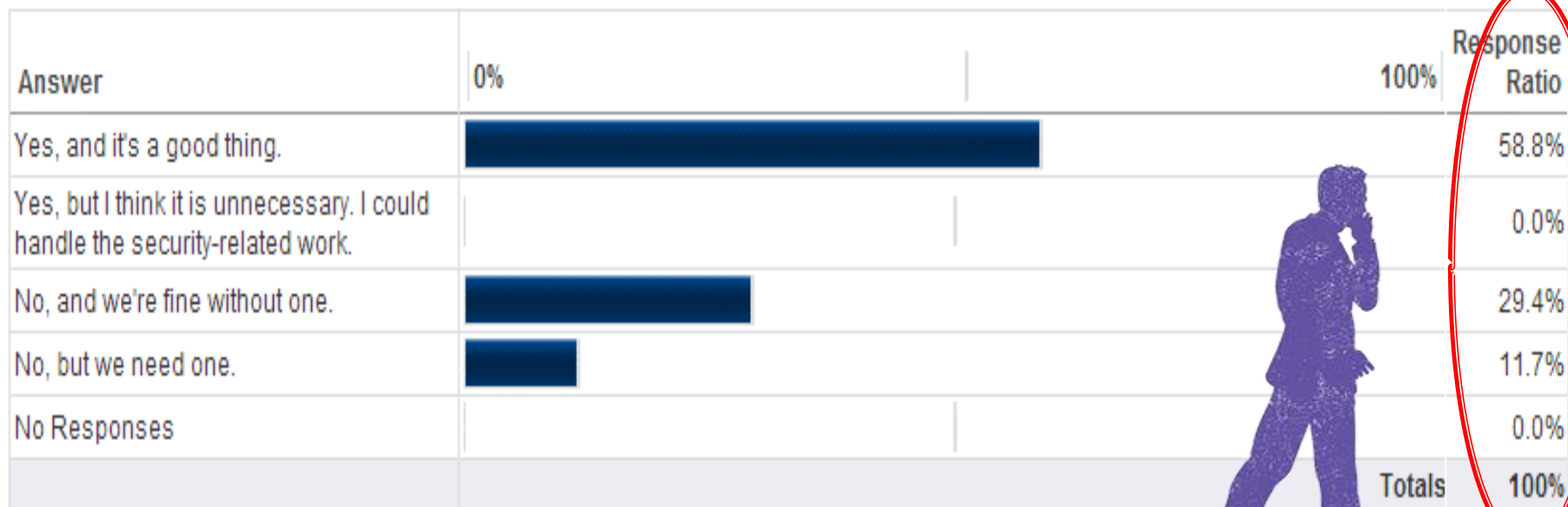


Moving Forward

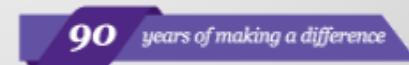


The Healthcare CISO is a Necessary Role, However Not All Organizations Are There Yet...

* Does your organization have a Chief Information Security Officer?



Source: <http://healthsystemcio.com/2014/06/26/survey/>



Where To Start To Have A Fighting Chance (Pre-Incident Response)

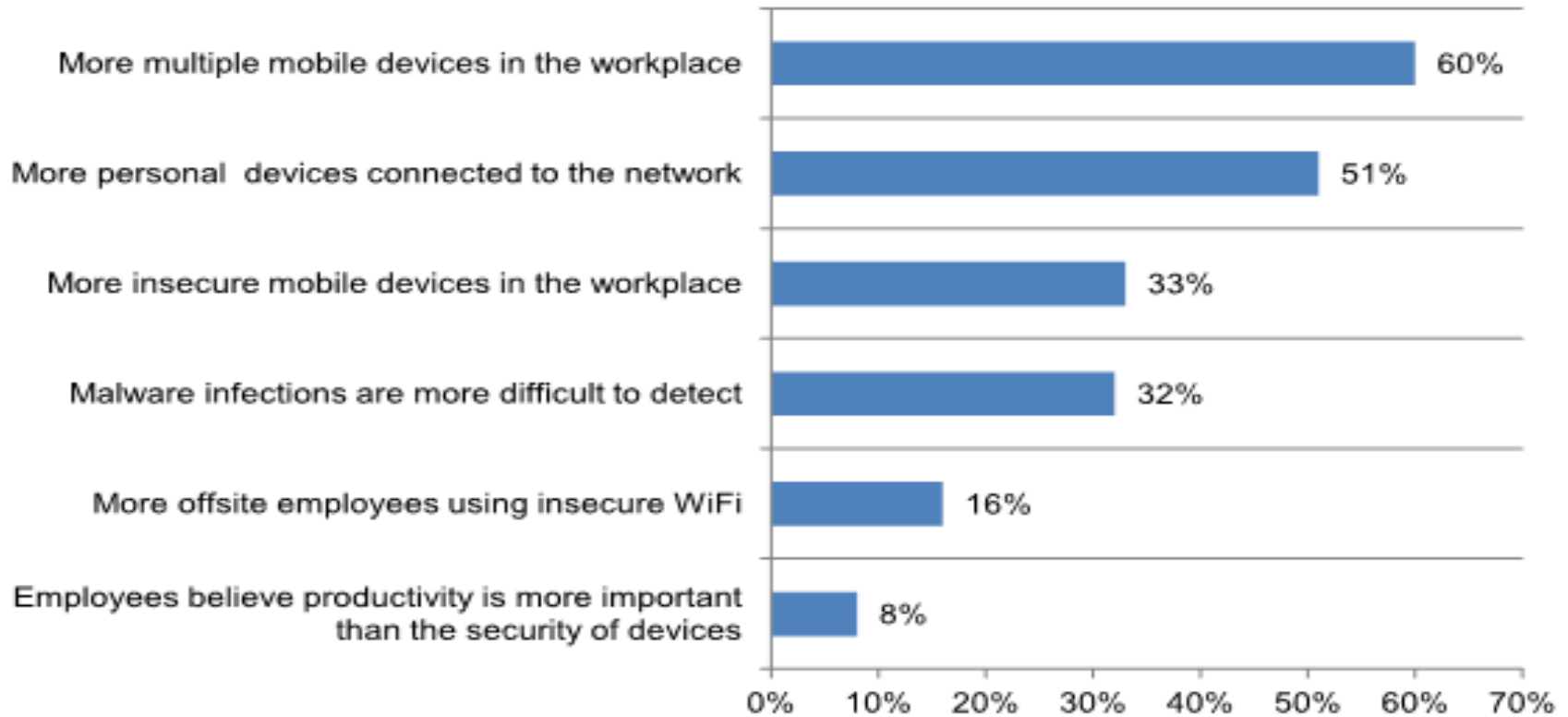
1. Risk Assessment
2. Asset Inventory/Tracking
3. Encrypt ALL Devices
4. Employee Training/Phishing Campaigns
5. Baseline Configurations
6. Vulnerability Assessment/Pen Testing
7. Monitoring for Anomalies
8. Admin Rights/Access Control
9. Vendor/Business Associate Management



Mobile Devices Becoming New Attack Point

Figure 1. What are the biggest threats to endpoint security?

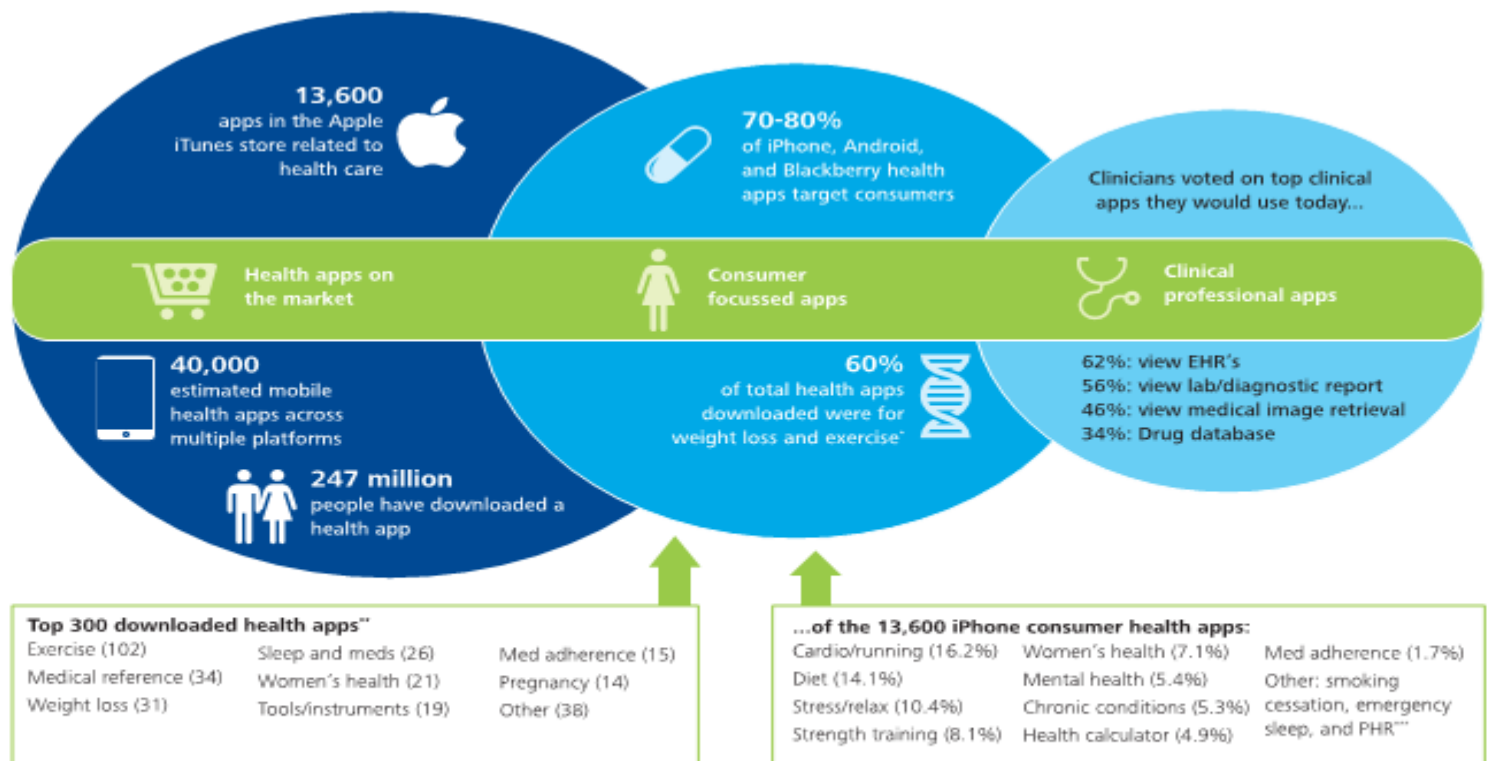
Two responses permitted



Source: 2014 State of the Endpoint, Ponemon Institute



40,000+ Healthcare Apps And Growing!



Source:

* As of March 2012, iPhone and Android combined Source: "Mobile Health Applications: 2012 study", Verasoni Worldwide, August 2012

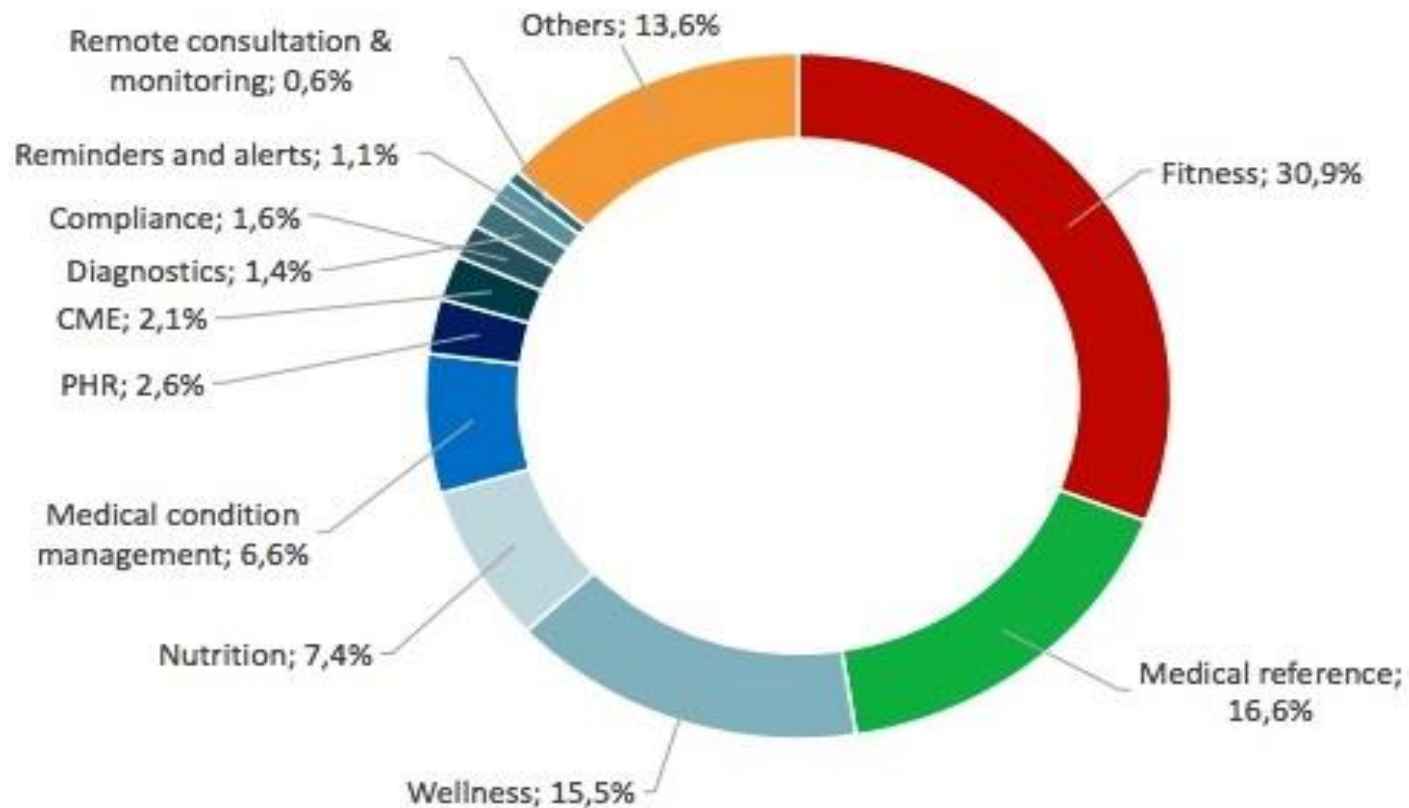
** Source: Dunbrack L. "The second wave of clinical mobility: Strategic solution investments for Mobile point of care", December 2011, IDC *Health insights*

*** PHR = personal health record. Source: "An analysis of consumer health apps for Apple's iPhone 2012," *Mobilehealthnews*, July 11, 2011



Fitness Is Largest Healthcare App Category

mHealth app category share



Source: research2guidance, 808 apps from Apple App Store, Google Play, BlackBerry App World and Windows Phone Store (March 2014)

Information Security Challenges (Mobile)



#1 Worry-
Lost/Stolen
Devices

#2 Worry 36%
forwarding to
cloud storage

42% Skip Malware
Scanning

**87% of Senior Managers
Send work to a home
computer or cloud to
work on remotely**

46% require power-on
password

Just 39% have MDM Systems in
Place, while 68% support BYOD



Source: Informationweek.com, 2014 Survey

Gartner 2015 Predictions - Is Healthcare Ready ?

2012	2013	2014	2015
Big data	Strategic big data	Smart machines	Smart machines
Extreme low-energy servers	Integrated ecosystems	Web-scale IT	Web-scale IT
Next generation analytics	Actionable analytics	3D printing	3D printing
App stores and marketplaces	Enterprise app stores	Software-defined anything	Software-defined applications/infrastructure
IoT	IoT	IoT	IoT
In-memory computing	In-memory computing	Cloud/client architecture	Cloud/client computing
Mobile-centric applications/interfaces	Mobile applications/HTML5	Mobile apps and applications	Risk-based security/self-protection
Cloud computing	Hybrid IT/cloud computing	Hybrid cloud & IT as a service broker	Advanced pervasive/invisible analytics
Media tablets and beyond	Mobile device battles	Mobile device diversity/management	Computing everywhere
Contextual/social user experience	Personal cloud	Era of the personal cloud	Content-rich systems

Source: <http://www.techrepublic.com/blog/10-things/gartners-top-10-technology-trends-for-2015-all-about-the-cloud/> (11/3/14)



Final Thoughts

- ▶ 2014 Started the "Sophisticated Malware Breach" narrative
- ▶ Accentuates the importance of:
 - Training
 - Information Security Governance
 - Blocking and tackling (security fundamentals)
 - Encrypting everywhere
- ▶ Increased investment is necessary
- ▶ 2 year monitoring, cyber insurance, being in front of the incident response becoming the norm



Suggested Breach References

- www.pcworld.com/article/2453400/the-biggest-data-breaches-of-2014-so-far.html
- online.wsj.com/articles/apple-celebrity-accounts-compromised-by-very-targeted-attack-1409683803
- <http://www.businessinsider.com/urban-outfitters-executive-data-breach-2014-8>
- <http://www.idtheftcenter.org/ITRC-Surveys-Studies/2014databreaches.html>
- <http://www.crn.com/slide-shows/security/300072686/the-error-of-your-ways-top-10-data-breaches-of-2014.htm/pgno/0/6>
- <http://announcements.ebay.com/2014/05/ebay-inc-to-ask-ebay-users-to-change-passwords/>
- <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html>
- <http://www.modernhealthcare.com/section/articles?tagID=5789>
- <http://www.washingtonpost.com/blogs/wonkblog/wp/2014/08/19/health-care-data-breaches-have-hit-30m-patients-and-counting/>
- <http://www.isaca.org/Knowledge-Center/Blog/Lists/Posts/Post.aspx?List=ef7cbc6d%2D9997%2D4b62%2D96a4%2Da36fb7e171af&ID=471>



THANKS MUCH AND GOOD LUCK IN 2015!!



Todd Fitzgerald

Global Information Security Director

Grant Thornton International, Ltd.

Oak Brook Terrace, IL

todd.fitzgerald@gti.gt.com



Grant Thornton

An instinct for growth™



Todd_fitzgerald@yahoo.com

[linkedin.com/in/toddfitzgerald](https://www.linkedin.com/in/toddfitzgerald)



hipaacow.org

Thank You!

Thank you for viewing this webinar. If you have any comments or feedback, please feel free to email us at admin2@hipaacow.org.

Visit our website at hipaacow.org!!



“Like Us” on



“Follow Us” on

