

An Analysis of Breaches Affecting 500 or More Individuals in Healthcare

August 2010

By Chris Hourihan

The passing of the **Health Information Technology for Economic and Clinical Health Act (HITECH) Act** in early 2009 as part of American Recovery and Reinvestment Act (ARRA) outlined a number of privacy and security provisions directly applicable to Covered Entities and Business Associates in the way of breach notification, extending the requirements of HIPAA, and increasing enforcement and penalties. Since that time, the provisions of the Act have been defined as new rules (HIPAA Breach Notification Interim Final Rule, 45 CFR Part 164 Subpart D¹) or as updates to existing rules². Section 164.408(b) of Subpart D requires that covered entities notify the HHS Secretary immediately of any breaches of unsecured PHI affecting 500 or more individuals, and that the Secretary make these breaches publicly known on the HHS website.

Since the HIPAA Breach Notification Rule took effect on September 23, 2009 through the publication of this analysis, **108 breaches** affecting approximately **4,089,670 individuals and health records** have been reported³. My initial analysis of this data took place in mid-May of 2010, at which time 69 breaches had been reported affecting some 1.6M records; in the span of three-and-a-half months, there were 39 new breaches affecting 2.43M records.

It is important to note that what constitutes a breach and is subsequently reported to the Secretary: an organization believes the incident “poses a significant risk of financial, reputational, or other harm to the individual;” this does not mean some form of harm has been enacted upon everyone or even anyone affected. While this provides the possibility for an organization to not notify individuals—if the organization performs a risk assessment and determines the risk of harm is significantly low—organizations appear to be erring on the side of caution and providing notice to the individuals and Secretary regardless. In one specific instance with Rainbow Hospice and Palliative Care, the laptop that was stolen was in fact encrypted, yet notice was still provided.

From a cost perspective, an annual study conducted by the Ponemon Institute⁴ finds that the average cost per compromised record is \$204—\$144 of indirect costs and \$60 of direct costs. That comes to a total cost of \$834.3M for all organizations; \$245.3M in direct costs to all organizations; and an average cost of \$7.7M—\$2.3M in direct costs.

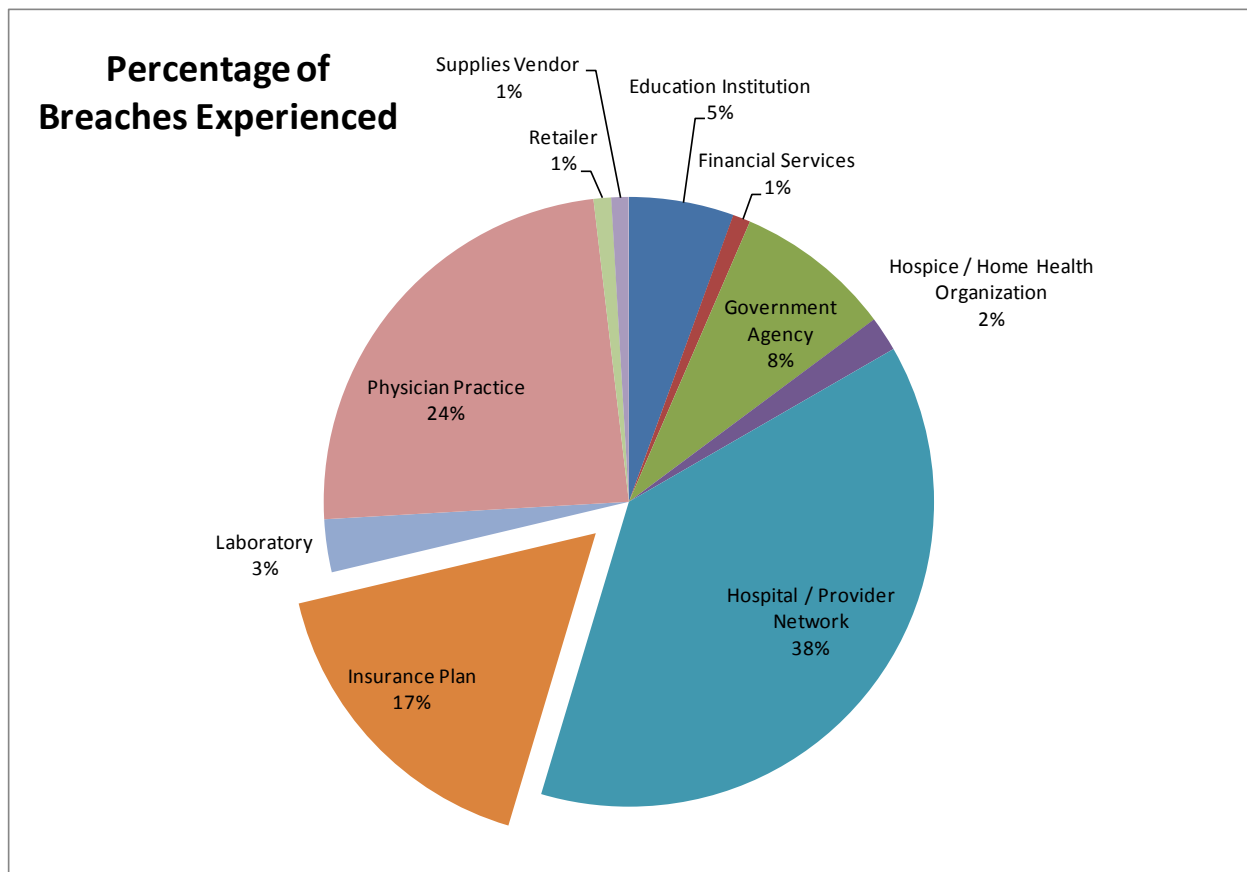
What follows is meant to serve as an analysis of the publicly available information to provide useful data points to professionals, security and non-security, in the healthcare industry. For a detailed breakdown of breach data for each area, please see the Appendix.

Breaches by Industry Segment

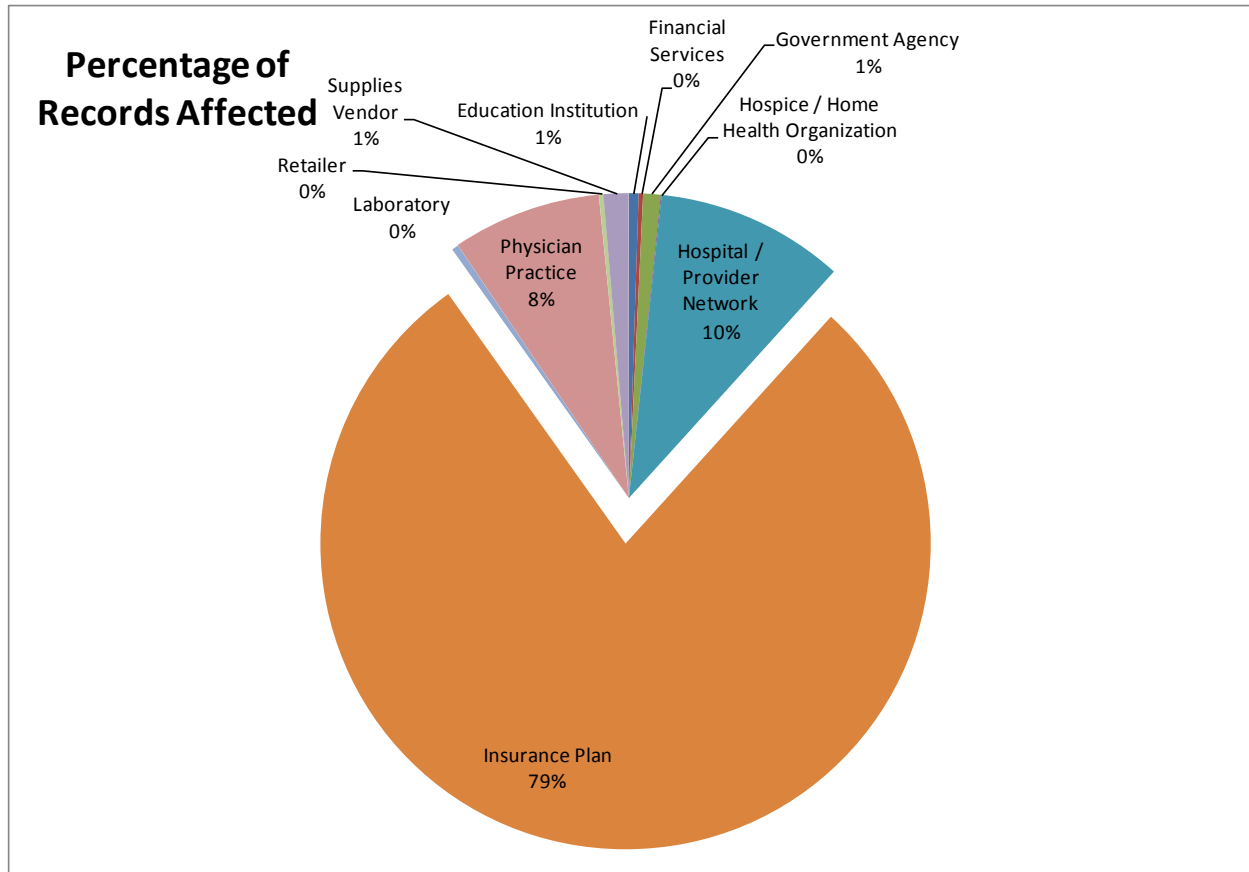
Based on the names listed, each organization is categorized into one of ten types:

- Education Institution
- Financial Services
- Government Agency
- Hospice / Home Health
- Hospital / Provider Network
- Insurance Plan
- Laboratory
- Physician Practice
- Retailer
- Supplies Vendor

Of these categories, Hospitals / Provider Networks experienced the highest number of breaches at 41, followed by Physician Practices with 26.



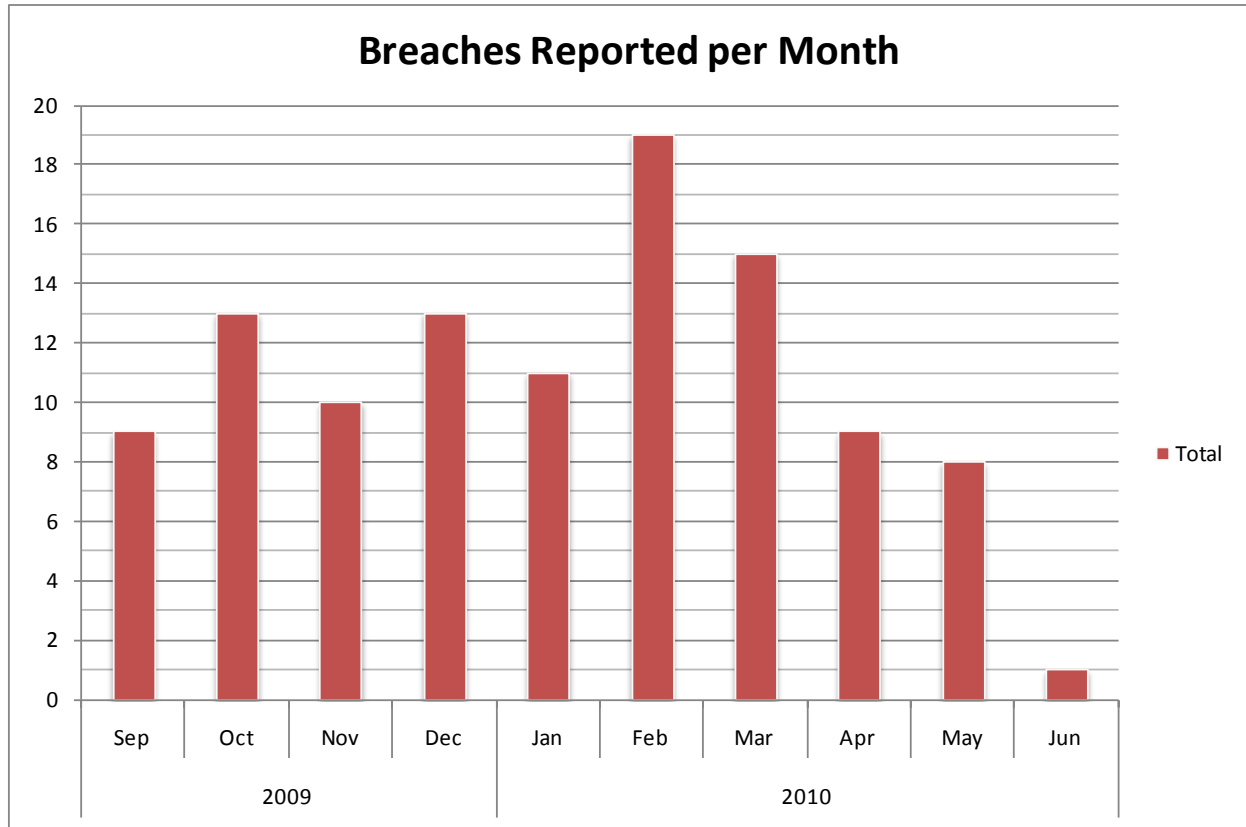
However, when looking at the number of individuals affected by the breaches, Insurance Plans make up the largest category accounting for 78% or 3.2M, of the records, while Hospitals / Provider Networks comprise only 10% or 408K, of the records.



Of the Top 10 largest breaches reported (see section Top 10 Breaches) Insurance Plans represent five of the ten for a total of 3.1M records, or 86% of the of the top 10.

Breaches Per Month

Since September, 2009, a total of 108 breaches have been reported to the Secretary and posted to HHS' website. On average, the healthcare industry is experiencing 10.8 breaches affecting 500 or more individuals per month. The month of February, 2010 saw the most breaches at 19.



The good news is that since February there is a downtrend in breaches per month, with only one being reported so far in June and none in yet for the month of July. However, one must consider that an organization has 60 days to report a breach, meaning breaches in June and July may still be reported.

Breaches by Type and Location

HHS collects and publishes two key points of data beyond the number of individuals affected by a particular breach: type and location.

Type represents the exploit or action, intentional and unintentional, which resulted in the breach. Location represents where the PHI was stored that was disclosed to an unauthorized individual. As a simple example of this, if an unencrypted laptop is stolen, the *laptop is the location* of the PHI and *theft is the type* of breach.

While HHS specifies its own locations, for the purposes of this analysis, location is distilled into fewer, more concise categories, which are:

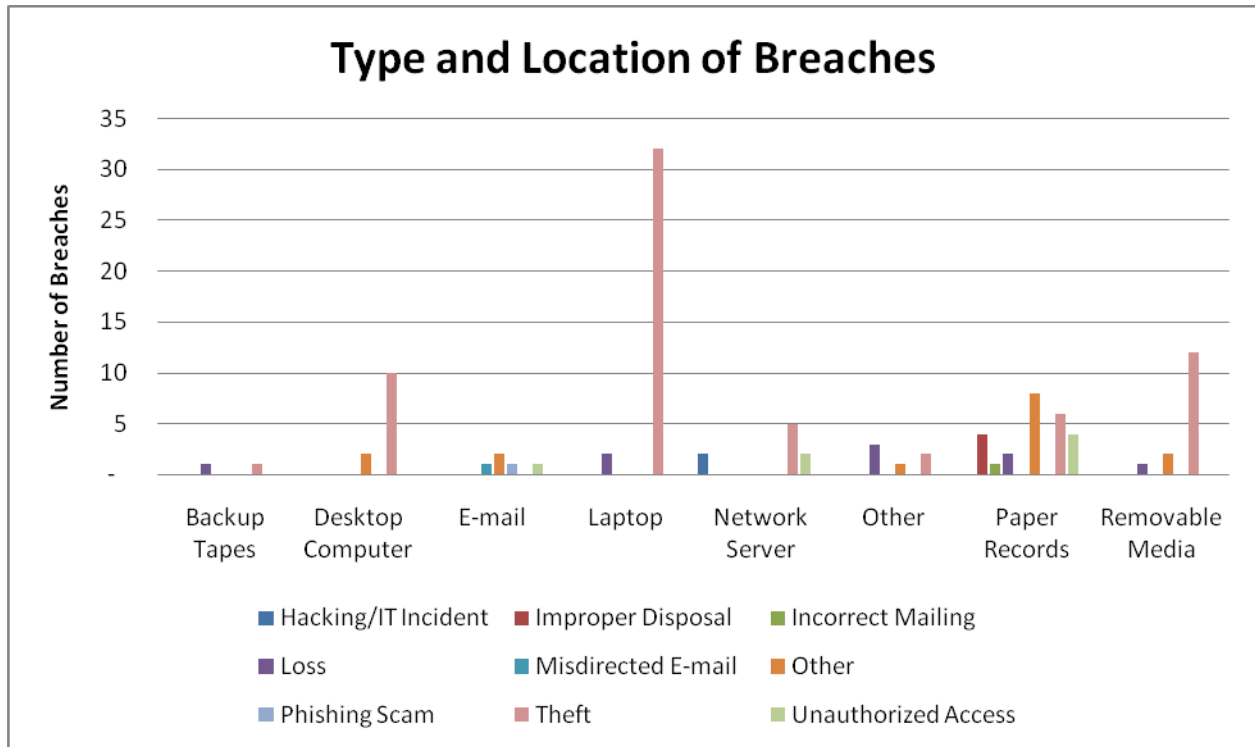
- Backup Tapes
- Desktop Computer
- E-mail
- Laptop
- Network Server
- Other
- Paper Records
- Removable Media (e.g., hard drives, USB drives)

The types of breaches are categorized as follows:

- Hacking/IT Incident
- Improper Disposal
- Incorrect Mailing
- Loss
- Misdirected E-mail
- Other
- Phishing Scam
- Theft
- Unauthorized Access

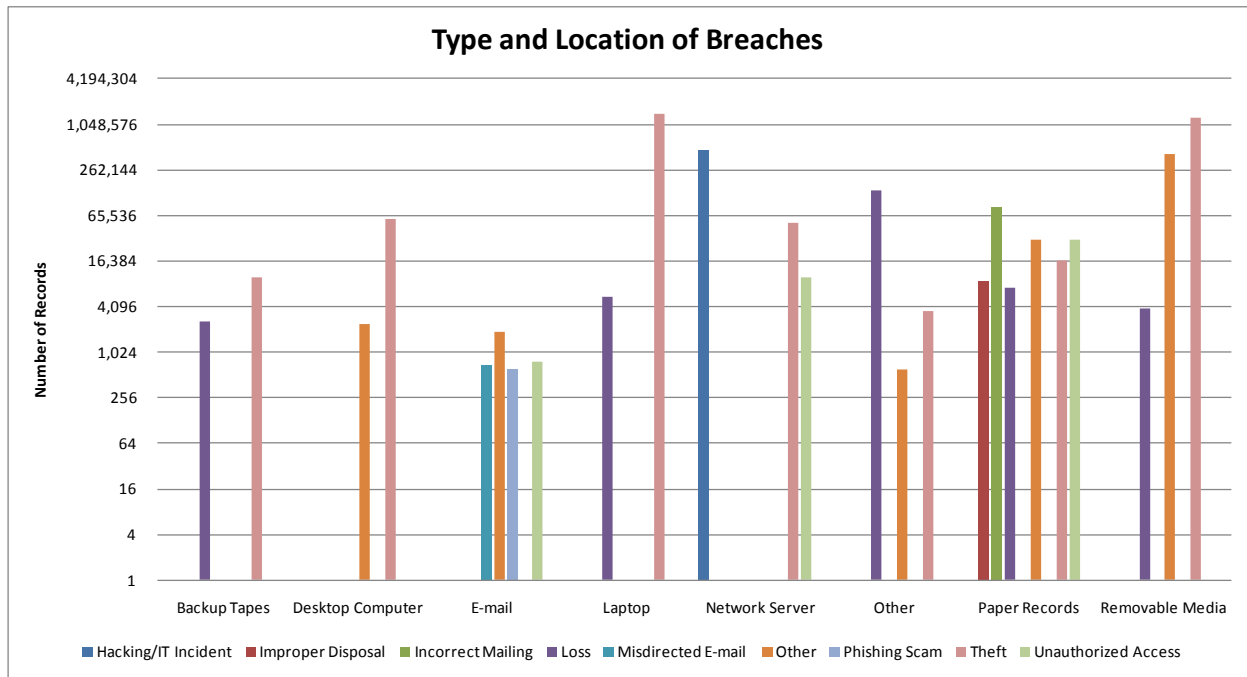
Looking at the cross-section of these categories and focusing first on simply the number of breaches experienced, the theft of laptops was the number one cause resulting in a total of 32 breaches reported. The next closest leading causes are theft of desktop computers and theft of removable media resulting in 10 and 12 breaches respectively. The total number of thefts reported is an astonishing 68 or 63% of all breaches.

Looking at the other axis, or location of the PHI, laptops were the biggest source with 34, or 31%, of all breaches. Paper records were the next leading location with 25 breaches.



Interesting, only two hacking incidents have been reported to date, and only one caused significant damage affecting some 480,000 records (see below).

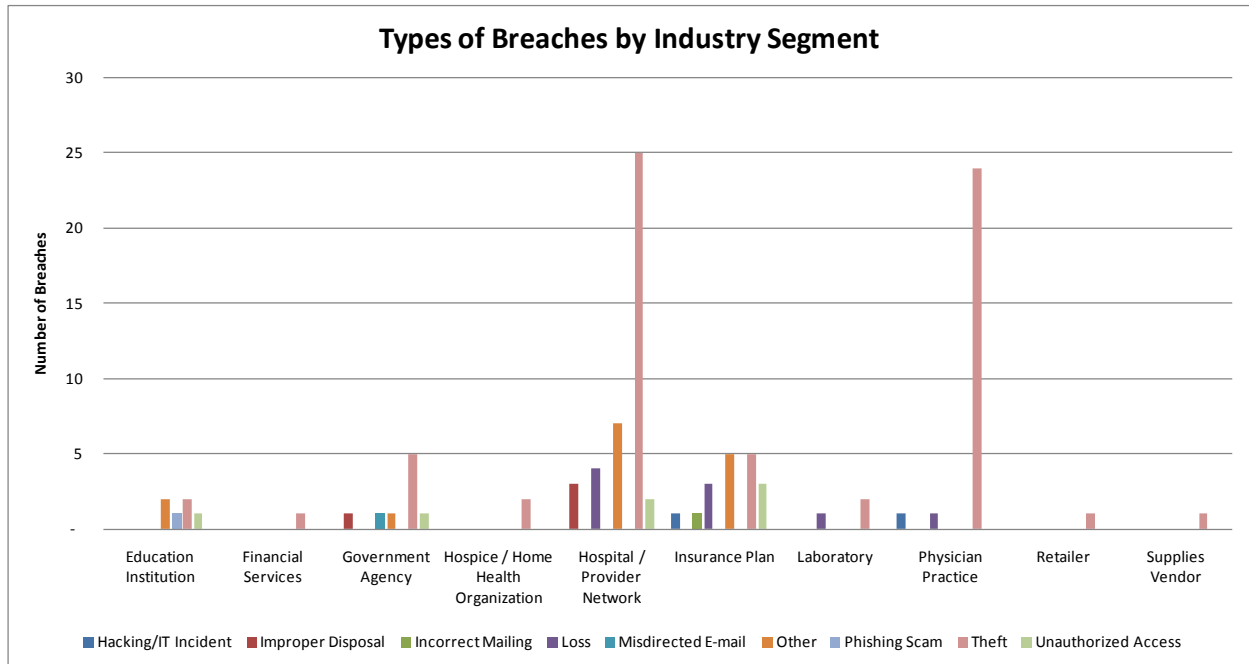
When looking at the number of individuals affected by each breach, the primary means again is theft with 2.8M or 70% of records. The primary locations are removable media and laptops with 1.7M and 1.45M respectively, or a combined 77%.



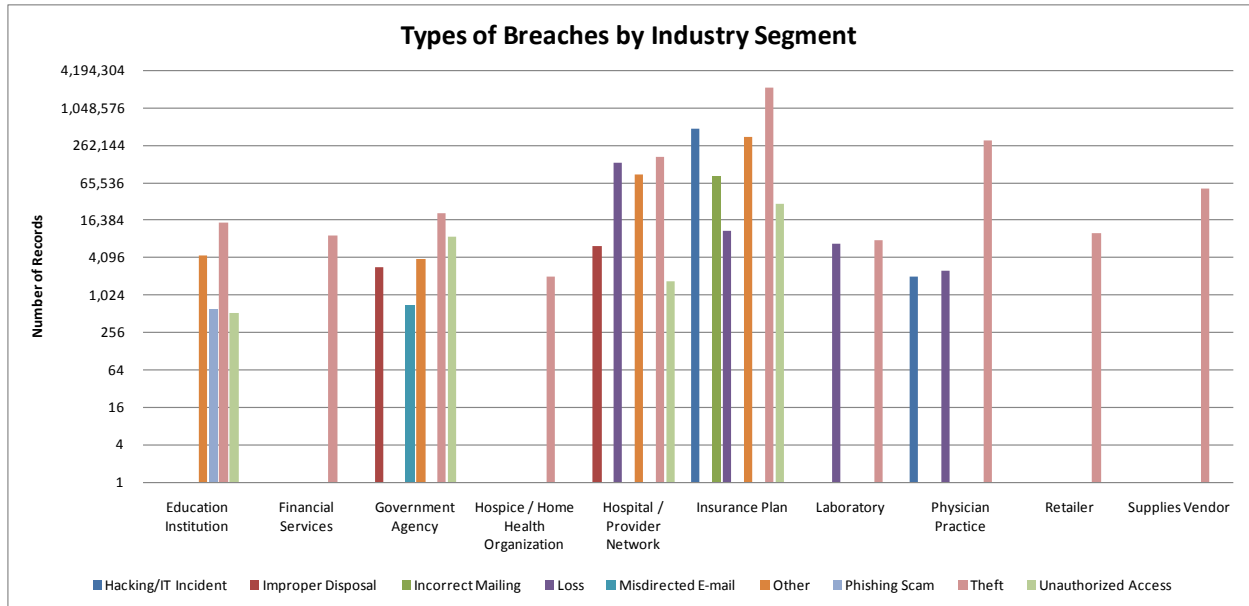
With so many records on laptops and removable media being breached, it is clear to see that better endpoint management, and more specifically encryption, solutions need to be implemented throughout organizations. The ROI is clear even when just looking at the direct costs for notification, with an organization on average paying \$3.85M when removable media or a laptop is lost or stolen (64K records breached on average times \$60 per record).

Breaches by Type and Industry Segment

In looking at the intersection of the industry segment and the type of breach, theft is the only type of breach experienced by every industry segment, accounting for 68 of the 108 breaches reported with Hospitals / Provider Networks and Physician Practices being the biggest targets with 25 and 24 thefts respectively.



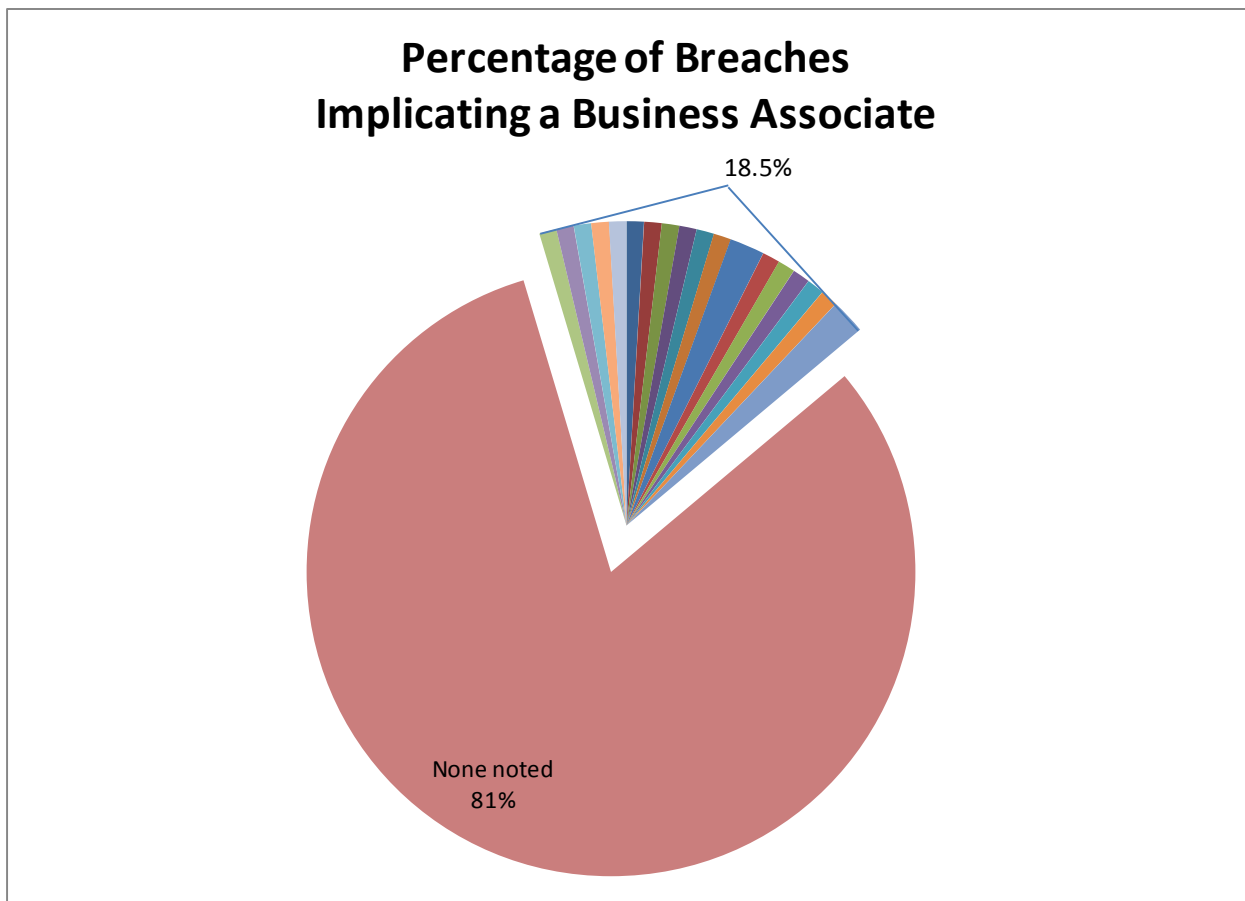
While Insurance Plans experienced relatively few theft breaches, due to the few high profile breaches in the Top 10 list (see section Top 10 Breaches), that segment by far experienced the worst losses with 2.2M records breached due to theft.



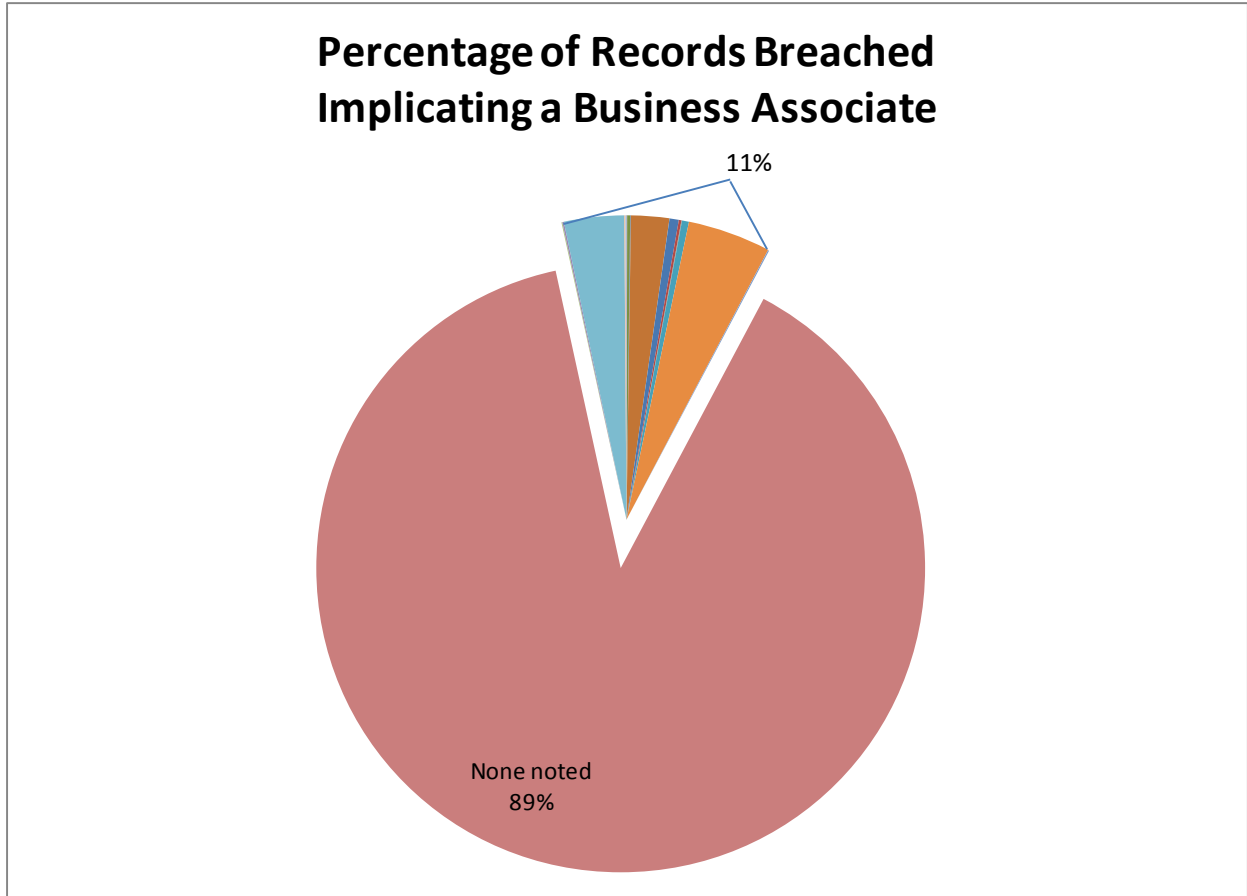
Breaches Involving Business Associates

The HITECH Act changed security in the healthcare industry by making Business Associates directly responsible for the provisions of the HIPAA Security, Privacy, and Breach Notification Rule. While the intent is sound as a means of increasing security throughout the chain of information sharing, it by no means lets covered entities off the hook in ensuring their Business Associates are implementing appropriate security. The Covered Entities, as is made clear on the HHS website, remain the primary parties responsible for the PHI and subsequently for the notification and associated costs. In fact it is recommended that Covered Entities require their Business Associates to provide notification much sooner than the 60 day deadline, and that Covered Entities play a role in the analysis of the breach.

Of the 108 breaches reported since September 2009, 20 or 18.5% implicated a Business Associate.

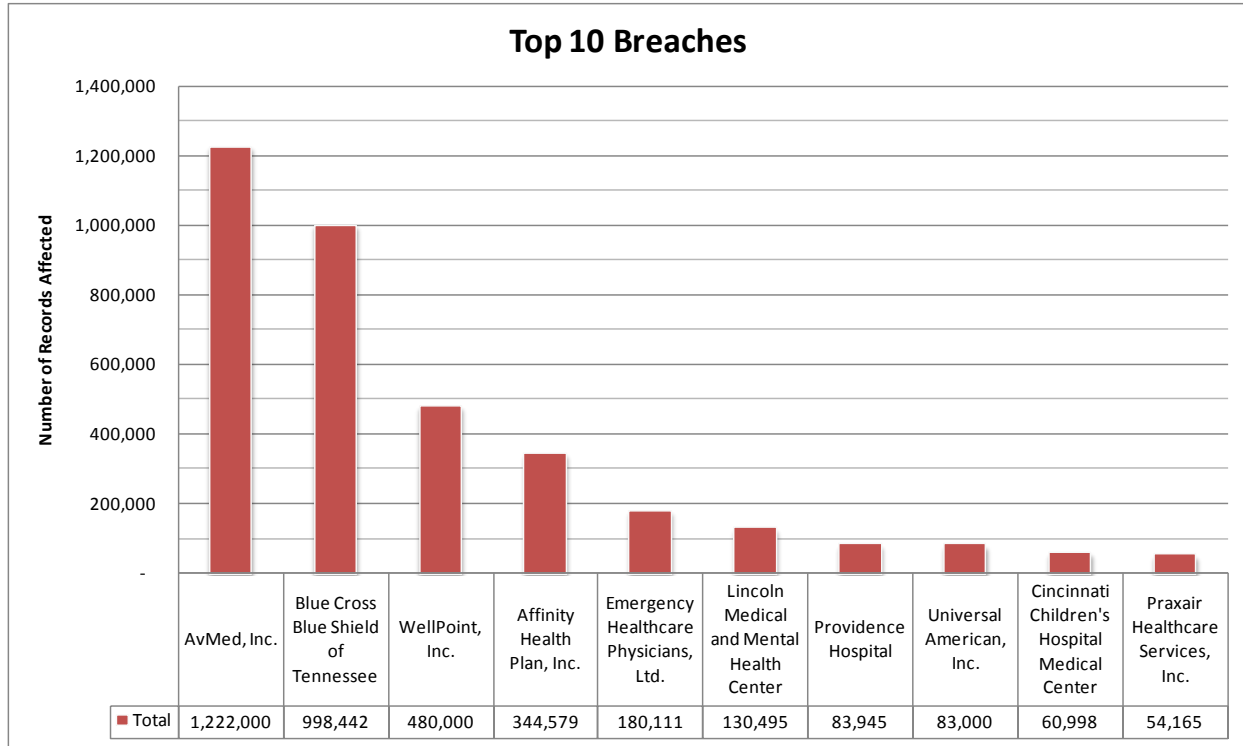


The 18.5% of breaches involving a Business Associate equates to 11% or 457K records accessed by an unauthorized individual.



Top 10 Breaches

Of the 108 breaches reported and 4.09M records affected, the top 10 represent 89% or 3.64M of the records breached.



Comments and Details

A requirement of the HITECH Act Breach Notification Rule is “to provide notice to prominent media outlets serving the State or jurisdiction” where a breach affects 500 or more individuals of a State or jurisdiction. While not every breach will require a media notification, a fair number have provided some form of public comment, which are detailed below by organization. Please note that this list only comprises those breaches listed since January 2010.

Organization Name	~# of Individuals Affected	Date of Breach	Type of Breach	Location of Breach Information (HHS Reported)	Comments
University Health System	7,526	June-10	Theft	Network Server	Two computer servers were stolen from the university health system's billing office in Reno. "For some patients of University Health System in northern Nevada, the information which may possibly have been viewed includes names, addresses, birth dates, social security numbers and medical information. In an abundance of caution, these patients will be offered a year of credit monitoring service at no cost." http://www.uhsnevada.org/uhs_news/app-news/121/
Private Practice	600	May-10	Theft	Network Server	No further details available to date.
Children's Hospital & Research Center at Oakland	1,000	May-10	Other	Paper	"Hospital officials determined that equipment designed to generate, fold and stuff documents for mailing was programmed to fold and stuff two pages rather than one. This programming error caused guarantor billing statements prepared on May 25 and May 26 to be collated and mailed incorrectly. As a result, approximately 1,000 guarantor statements mailed included a second page that contained the guarantor statement for another person." http://www.childrenshospitaloakland.org/EnhancedPatientPrivacyProtection.asp
Private Practice	5,983	May-10	Theft	Laptop	No further details available to date.
Occupational	1,105	May-10	Theft	Laptop	No further details available to date.

Health Partners Oconee Physician Practices	653	May-10	Theft	Laptop	"A laptop containing information on more than 600 patients at an Oconee County physicians' practice was stolen...The laptop was dedicated for use with an EKG machine and...connected to the hospital's main IT network." http://www.phiprivacy.net/?tag=oconee-heart-center
	4,083	May-10	Improper Disposal	Paper Records	"...a binder and clipboard containing patient names, social security numbers and dates of birth of approximately 4,038 outpatients from February 1 through April 23 were recently found to be missing from a secured-access laboratory area." http://www4.va.gov/ABOUT_VA/docs/Dallas_media_notice1.pdf
VA North Texas Health Care System	937	May-10	Other	E-mail	No further details available to date.
	2,300	May-10	Theft	Laptop	No further details available to date.
Sinai Hospital of Baltimore, Inc. Private Practice	1,020	April-10	Theft	Laptop	No further details available to date.
	1,001	April-10	Unauthorized Access	Desktop Computer Network Server	"...an unencrypted list of patient names and addresses was sent via e-mail from the hospital to a local not-for-profit agency for use in a summer camp mailing. The list contained the names and addresses of patients who were treated in two clinics during a 15-month period. " http://www.childrensdayton.org/cms/media_releases/9e1ed1a53f9b284f/index.html
Comprehensive Care Management Corporation	1,001	April-10	Other	E-mail	http://www.childrensdayton.org/cms/media_releases/9e1ed1a53f9b284f/index.html
	656	April-10	Theft	Laptop	"On April 22, an unencrypted laptop belonging to VA contractor Heritage Health Solutions was stolen from a vehicle, compromising the records of more than 600 veterans...Heritage Health Solutions has 69 contracts with VA, and 25 of those don't have clauses requiring personal data to be encrypted..." http://www.phiprivacy.net/?tag=heritage-health-solutions
The Children's Medical Center of Dayton	1,745	April-10	Loss	Laptop	No further details available to date.
	2,628	April-10	Other	Paper	"...an envelope stuffing machine was placing two bills in each
Veterans Health Administration					
St. Jude Children's Research Hospital University of					

Rochester Medical Center Affiliates				Records	envelope, resulting in patients getting an extra bill intended for someone else...As a result, about half of the 2,500 bills Strong Memorial Hospital in Rochester, N.Y., mailed to patients on April 19 went to the wrong patient." http://www.healthcareinfosecurity.com/articles.php?art_id=2559
Rainbow Hospice and Palliative Care	1,000	April-10	Theft	Laptop	"...a laptop computer containing patients' personal information was stolen during a nurse's home visit in April. The computer contained patient names, addresses, social security numbers, insurance information, medications, treatments and diagnoses, the health care provider said. 'The laptop was encrypted'" http://www.phiprivacy.net/?tag=rainbow-hospice-and-palliative-care
Loma Linda University Health Care	584	April-10	Theft	Desktop Computer	"A desktop computer containing the information disappeared April 5 from the department of surgery's administrative office...The missing information includes each patient's name, medical record number, diagnosis, surgery date, and the type of procedure." http://www.phiprivacy.net/?p=2802
Private Practice Silicon Valley Eyecare Optometry and Contact Lenses	4,200	April-10	Theft	Laptop	No further details available to date.
	40,000	April-10	Theft	Network Server	"...two burglars broke an outside window to the administrative area...confiscating the computer, and pushing the computer and a plasma TV back out the window of entrance...The server that was stolen contained our patient data base information. The patient records contain names, addresses, phone numbers, and in some cases social security numbers. E-mail addresses birthdates, family members, medical insurances as well as medical and ocular health information was included." http://www.databreaches.net/?p=11688
Our Lady of Peace Hospital	24,600	March-10	Theft	Portable Electronic Device	A flash drive containing some of their most personal and important information has been missing for more than a month. http://www.esecurityplanet.com/news/article.php/3880471/Hospital-Data-Breach-in-Kentucky-Affects-Thousands.htm
Cincinnati Children's Hospital Medical	60,998	March-10	Theft	Laptop	"The theft [of a password-protected laptop computer containing information regarding 61,027 patients] occurred from an employee's vehicle parked at his residence..."

Center					http://www.cincinnatichildrens.org/about/news/release/2010/stolen-laptop-05-28-2010.htm
Georgetown University Hospital	2,416	March-10	Theft	Portable Electronic Device	"The hard drive, stolen in late March, contained information on more than 2,400 patients at Georgetown University Hospital...The device contained reports from the hospital's surgery department, including patient name, date of birth, gender, date of surgery, type of surgery or test and medical record number." http://www.healthcareinfosecurity.com/articles.php?art_id=2563
Lincoln Medical and Mental Health Center	130,495	March-10	Loss	Other	"...seven CDs a business associate FedEx'd were lost..." http://www.healthdatamanagement.com/news/breach-notification-lincoln-medical-40601-1.html
Medical Center at Bowling Green	5,418	March-10	Theft	Portable Electronic Device	"Theft of computer equipment from The Medical Center's Mammography Suite containing the information of patients...The information on the hard drive was not encrypted; however, the harddrive was maintained in a locked, non-public, private area." http://www.mcbg.org/pdf/Breachv12.pdf
TennCare	10,515	March-10	Theft	Laptop	"A laptop was in the trunk of a vehicle that was stolen on March 20 in Chicago. The vehicle belonged to an employee of a subcontractor to DentaQuest...The computer was password protected but did not have any other safeguards to prevent unauthorized access to the information." http://www.scmagazineus.com/laptop-theft-puts-thousands-of-nm-medicaid-users-at-risk/article/170118/
State of New Mexico Human Services Department, Medical Assistance Division	9,600	March-10	Theft	Laptop	"A laptop was in the trunk of a vehicle that was stolen on March 20 in Chicago. The vehicle belonged to an employee of a subcontractor to DentaQuest...The computer was password protected but did not have any other safeguards to prevent unauthorized access to the information." http://www.scmagazineus.com/laptop-theft-puts-thousands-of-nm-medicaid-users-at-risk/article/170118/
Beatrice Community Hospital and Health Center	660	March-10	Other	Paper Records	No further details available to date.

Tomah Memorial Hospital	600	March-10	Other	Other	Nurse misused her legitimate access to protected health information. The nurse is charged with fraudulently obtaining controlled substances between April 2008 and March 2010. http://www.tomahjournal.com/articles/2010/04/24/news/03breach.txt
Rockbridge Area Community Services	500	March-10	Theft	Laptop	"...six computers were stolen from a fire damaged building...where mental health, substance abuse, and prevention services were offered...as of April 23, 2010, three computers were recovered..." http://www.racsb.org/pages/documents/HIPAA_BreachNotice.pdf
University of Pittsburgh Student Health Center	8,000	March-10	Theft	Desktop Computer Paper Records	No further details available to date.
Mount Sinai Medical Center	2,600	March-10	Theft	Laptop	An unencrypted laptop computer containing hearing test information on about 2,600 newborns was stolen. http://www.healthcareinfosecurity.com/articles.php?art_id=2418
St. Joseph Heritage Healthcare	22,012	March-10	Theft	Desktop Computer	"St. Jude Heritage Medical Group in Fullerton has notified about 22,000 patients that their personal health and financial data might have been accessed after five computers were stolen." http://www.databreaches.net/?p=11455
Hypertension, Nephrology, Dialysis and Transplantation, PC	2,024	March-10	Theft	Laptop	No further details available to date.
Emergency Healthcare Physicians, Ltd.	180,111	March-10	Theft	Portable Electronic Device	"...the records were on a portable hard drive and stolen from the Westmont office of Millennium Medical Management Resources." http://www.phiprivacy.net/?tag=emergency-healthcare-physicians
Blue Cross & Blue Shield of Rhode Island	12,000	February-10	Unauthorized Access	Paper Records	"...personal information belonging to approximately 12,000 BlueCHIP for Medicare members was inadvertently contained in a filing cabinet donated with other surplus office furniture to a local nonprofit organization." https://www.bcbsri.com/BCBSRIWeb/about/newsroom/news_releases/2010/MemberInfoBreach.jsp

Montefiore Medical Center Private Practice	625	February-10	Theft	Laptop	No further details available to date.
	21,000	February-10	Theft	Portable Electronic Device	No further details available to date.
Massachusetts Eye and Ear Infirmary	3,594	February-10	Theft	Laptop	"...a laptop belonging to a physician affiliated with the Massachusetts Eye and Ear Infirmary was stolen while the physician was lecturing in South Korea...laptop contained demographic and health information of approximately 3,526 patients." http://www.masseyeandear.org/news/press_releases/recent/lapt-op-data-breach/
Praxair Healthcare Services, Inc.	54,165	February-10	Theft	Laptop	"...theft of a company computer whose hard drive contained certain client names and other personal or health-related information." http://www.praxair.com/praxair.nsf/AllContent/87CA1B900551E83D8525770A005FD3A8?OpenDocument
Laboratory Corporation of America/US LABS/Dianon Systems, Inc.	2,773	February-10	Theft	Portable Electronic Device	No further details available to date.
South Carolina Department of Health and Environmental Control	2,850	February-10	Improper Disposal	Paper Records	"...private information of more than 1,800 people was included on DHEC documents that were discovered by a third party in a public, paper recycling container behind the DHEC building..." http://www.phiprivacy.net/?p=2528
North Carolina Baptist Hospital	554	February-10	Theft	Paper Records	A bag containing documents with the patient information was stolen Feb. 15 from an employee's locked car in the parking deck of an off-campus outpatient clinic. http://www.securityinfowatch.com/Healthcare+Facilities/1315330
Laboratory Corporation of America/Dynacare	5,080	February-10	Theft	Laptop	No further details available to date.

Northwest, Inc. Pediatric Sports and Spine Associates	955	February-10	Theft	Laptop	"...a laptop computer used by Pediatric Sports and Spine Associates was stolen from one of our employees. This laptop computer may have contained some patient information, including name, address, phone number, date of birth, and social security number, as well as limited information about patient treatment or medication." http://www.pedibones.com/PediatricSportsandSpineNotice.pdf
Reliant Rehabilitation Hospital of North Houston	763	February-10	Unauthorized Access	E-mail	An email correspondence, sent by CPSI was unintentionally sent to an unauthorized individual. The personal information included was limited in nature; including; patient name, dates of service, the last 4 digits of the account #, total charges, account balance, length of stay, insurance payer classification and service type. http://www.reliantnorthhouston.com/pdf/breach-letter.pdf
University of New Mexico Health Sciences Center	1,900	February-10	Other	Desktop Computer	Two stand alone computers in a small, off-site clinic were infected with malware. The file contained the names and other limited personal information of approximately 1,900 patients treated in that facility between 2007 and 2009. http://hsc.unm.edu/safeguards/background.shtml
General Agencies Welfare Benefits Program	1,874	February-10	Loss	Other	"Two DVDs sent the first week of February 2010, between two Towers Watson office locations, were lost in transit...The DVDs contained personal data and health insurance plan information regarding certain general agency and other employees, former employees, and their family members covered by the program." http://www.gcfa.org/PressReleases/2010/Towers Waters Website Notification 4-27-10r.pdf
Providence Hospital	83,945	February-10	Other	Hard Drives	A hard drive used for backing up data has been "lost or stolen from a locked office suite." http://www.clickondetroit.com/health/23070110/detail.html
John Muir Physician Network	5,450	February-10	Theft	Laptop	Two laptop computers were stolen at the John Muir Physician Network Perinatal office in Walnut Creek. "The laptops were password protected and contained data in a format that would not be readily accessible. While we have no evidence that the information has been accessed or used inappropriately, we cannot

					rule out that possibility, and, therefore, are notifying patients to help protect their identity,” said Hala Helm, Muir’s vice president and chief compliance and privacy officer. http://www.bizjournals.com/sanfrancisco/stories/2010/04/05/daily9.html
Griffin Hospital	957	February-10	Unauthorized Access Hacking/IT Incident	Network Server	A radiologist previously, but not currently, affiliated with the hospital or on the Griffin Hospital Medical Staff accessed patient radiology reports on the hospital's Digital Picture Archiving and Communication System (PACS) using the passwords of other radiologists and an employee within the Radiology Department. The passwords were obtained and/or used without their knowledge. http://www.griffinhealth.org/NewsEvents/NewsReleases/StoryDetail.aspx?id=5846
PMC Medicare Choice	605	February-10	Other	Paper Records	No further details available to date.
MMM Health Care Inc.	1,907	February-10	Other	Paper Records	No further details available to date.
City of Charlotte Health Plan	5,220	February-10	Loss	Other	"Two DVDs containing the sensitive information failed to arrive at the offices of Towers Watson & Co., the city's benefits consulting firm, based in Atlanta. The city of Charlotte was notified of the lapse on Feb. 23 and has blamed a mail-service provider working with Towers Watson." http://www.scmagazineus.com/charlotte-nc-notifies-thousands-of-city-workers-of-data-loss/article/171144/
Lee Memorial Health System	3,800	January-10	Other	Paper Records	No further details available to date.
Thrivent Financial for Lutherans	9,500	January-10	Theft	Laptop	Experienced a break-in at one of its offices in Pennsylvania and a laptop computer was among the items stolen. The laptop had a variety of safeguards to protect sensitive information, including strong password protection and encryption. http://www.businesswire.com/portal/site/home/permalink/?ndmViewId=news_view&newsId=20100309006450&newsLang=en
Shands at UF	12,580	January-10	Theft	Laptop	A Shands employee had downloaded the Health information onto an unencrypted Shands-owned laptop at home for work-related

					purposes. The employee reported the computer stolen on Jan. 27 when the employee's home was burglarized. http://www.businesswire.com/portal/site/home/permalink/?ndmViewId=news_view&newsId=20100309006450&newsLang=en
UnitedHealth Group Miami VA Healthcare System	16,291	January-10	Other	Paper Records	No further details available to date.
	568	January-10	Loss	Paper Records	"...a paper copy of a pharmacy log book containing the full name and partial Social Security number of some Veterans was reported missing by a member of our staff. Other information of a more personal nature, such as the date of birth or health information was not included in the log book." The log book was later recovered. http://www4.va.gov/ABOUT_VA/docs/MiamiVAHS.pdf
VA Eastern Colorado Health Care System	649	January-10	Improper Disposal	Paper Records	"...the personal health information, name, full and a few with partial Social Security numbers of some Veterans was left unattended in the Employee's Parking Garage in December of 2009." http://www4.va.gov/ABOUT_VA/docs/EasternColoradoPressRelease.pdf
The Methodist Hospital	689	January-10	Theft	Desktop Computer	A thief took the laptop on January 18. The computer was attached to a medical device that tests pulmonary function and contained private health information and Social Security numbers. http://abclocal.go.com/ktrk/story?section=news/local&id=7240553
Carle Clinic Association	1,300	January-10	Theft	Paper Records	No further details available to date.
Lucile Packard Children's Hospital	532	January-10	Other	Desktop Computer	No further details available to date.
Ashley and Gray DDS	9,309	January-10	Theft	Desktop Computer	A burglar stole a desktop computer from their dental practice. http://community.pennweldentalgroup.com/forum/topics/hhs-reports-a-missouri-dental
VHS Genesis Lab Inc.	6,800	January-10	Loss	Paper Records	No further details available to date.

Appendix A – Breaches by Industry Segment

Industry Segment	# of Individuals Affected
Education Institution	20,966
Financial Services	9,500
Government Agency	37,852
Hospice / Home Health Organization	2,020
Hospital / Provider Network	408,541
Insurance Plan	3,208,933
Laboratory	14,653
Physician Practice	323,040
Retailer	10,000
Supplies Vendor	54,165
Grand Total	4,089,670

Industry Segment	# of Breaches
Education Institution	6
Financial Services	1
Government Agency	9
Hospice / Home Health Organization	2
Hospital / Provider Network	41
Insurance Plan	18
Laboratory	3
Physician Practice	26
Retailer	1
Supplies Vendor	1
Grand Total	108

Appendix B – Breaches Reported per Month

Month	# of Individuals Affected
2009	
September	27,317
October	1,048,361
November	922,913
December	1,285,274
2010	
January	62,018
February	206,217
March	460,549
April	52,834
May	16,661
June	7,526
Grand Total	4,089,670

Month	# of Breaches
2009	
September	9
October	13
November	10
December	13
2010	
January	11
February	19
March	15
April	9
May	8
June	1
Grand Total	108

Appendix C – Breaches by Type and Location

	Backup Tapes	Desktop Computer	E-mail	Laptop	Network Server	Other	Paper Records	Removable Media	Grand Total
Hacking/IT Incident					482,000				482,000
Improper Disposal							9,012		9,012
Incorrect Mailing							83,000		83,000
Loss	2,562			5,545		137,589	7,368	3,800	156,864
Misdirected E-mail			676						676
Other		2,432	1,938			600	30,791	428,524	464,285
Phishing Scam			610						610
Theft	10,000	58,571		1,441,905	52,626	3,576	16,553	1,268,321	2,851,552
Unauthorized Access			763		9,980		30,928		41,671
Grand Total	12,562	61,003	3,987	1,447,450	544,606	141,765	177,652	1,700,645	4,089,670

	Backup Tapes	Desktop Computer	E-mail	Laptop	Network Server	Other	Paper Records	Removable Media	Grand Total
Hacking/IT Incident					2				2
Improper Disposal							4		4
Incorrect Mailing							1		1
Loss	1			2		3	2	1	9
Misdirected E-mail			1						1
Other		2	2			1	8	2	15
Phishing Scam			1						1
Theft	1	10		32	5	2	6	12	68
Unauthorized Access			1		2		4		7
Grand Total	2	12	5	34	9	6	25	15	108

Appendix D – Breaches by Type and Industry Segment

	Hacking / IT Incident	Improper Disposal	Incorrect Mailing	Loss	Misdirected E-mail	Other	Phishing Scam	Theft	Unauthorized Access	Grand Total
Education Institution						4,528	610	15,300	528	20,966
Financial Services								9,500		9,500
Government Agency		2,850			676	3,900		21,403	9,023	37,852
Hospice / Home Health Organization								2,020		2,020
Hospital / Provider Network		6,162		136,608		88,675		175,376	1,720	408,541
Insurance Plan	480,000		83,000	10,894		367,182		2,237,457	30,400	3,208,933
Laboratory				6,800				7,853		14,653
Physician Practice				2,562				318,478		323,040
Retailer	2,000							10,000		10,000
Supplies Vendor								54,165		54,165
Grand Total	482,000	9,012	83,000	156,864	676	464,285	610	2,851,552	41,671	4,089,670

	Hacking / IT Incident	Improper Disposal	Incorrect Mailing	Loss	Misdirected E-mail	Other	Phishing Scam	Theft	Unauthorized Access	Grand Total
Education Institution						2	1	2	1	6
Financial Services								1		1
Government Agency		1			1	1		5	1	9
Hospice / Home Health Organization								2		2
Hospital / Provider Network		3		4		7		25	2	41
Insurance Plan	1		1	3		5		5	3	18
Laboratory				1				2		3
Physician Practice	1			1				24		26
Retailer								1		1
Supplies Vendor								1		1
Grand Total	2	4	1	9	1	15	1	68	7	108

Appendix E – Breaches Involving a Business Associate

Business Associate Involved	# of Individuals Affected
Aramark Healthcare Support Services, Inc.	937
Blue Cross Blue Shield Rhode Island	528
Cogent Healthcare, Inc.	6,400
Computer Program and Systems, Inc	763
Deboer & Associates	800
Democracy Data & Communications, LLC	83,000
DentaQuest	20,115
Health Behavior Innovations	5,700
Heritage Health Solutions	656
McKesson Information Solutions, LLC	660
Merkle Direct Marketing	15,000
Millennium Medical Management Resources, Inc.	180,111
MSO of Puerto Rico, Inc.	2,512
Rick Lawson, Professional Computer Services	2,000
Service Benefits Plan Administrative Services Corp.	3,400
Siemens Medical Solutions, USA, Inc.	130,495
Towers Watson	1,874
United Micro Data	2,562
Grand Total	457,513

Business Associate Involved	# of Breaches
Aramark Healthcare Support Services, Inc.	1
Blue Cross Blue Shield Rhode Island	1
Cogent Healthcare, Inc.	1
Computer Program and Systems, Inc	1
Deboer & Associates	1
Democracy Data & Communications, LLC	1
DentaQuest	2
Health Behavior Innovations	1
Heritage Health Solutions	1
McKesson Information Solutions, LLC	1
Merkle Direct Marketing	1
Millennium Medical Management Resources, Inc.	1
MSO of Puerto Rico, Inc.	2
Rick Lawson, Professional Computer Services	1
Service Benefits Plan Administrative Services Corp.	1
Siemens Medical Solutions, USA, Inc.	1
Towers Watson	1
United Micro Data	1
Grand Total	20

References

1. "HIPAA Breach Notification Interim Final Rule, 45 CFR Part 164 Subpart D," U.S. Department of Health and Human Services,
<http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveridentities/breachnotificationifr.html>
2. "Notice of Proposed Rulemaking to Implement HITECH Act Modifications," U.S. Department of Health and Human Services,
<http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveridentities/hitechnprm.html>
3. "Breaches Affecting 500 or More Individuals," U.S. Department of Health and Human Services,
<http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/postedbreaches.html>
4. "2009 Annual Study: Cost of a Data Breach," Ponemon Institute LLC, January 2010,
http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/US_Ponemon_CODB_09_012209_sec.pdf

Author:

Christopher Hourihan, Manager, CSF Development and Operations, HITRUST
christopher.hourihan@hitrustalliance.net

The views expressed in this publication are the authors' alone, and do not reflect the views of any organizations with which they work. This is a publication of HITRUST Alliance providing general news about developments about information security in healthcare and should not be construed as providing legal advice, legal opinions or consultative direction.