COST OF A BREACH MODEL SUMMARY

Annual Revenues	**$ 250,000,000**
# of records breached	**10,000**

COST CATEGORY	COST IMPACT	COST SUB-CATEGORY	COST	TOTAL COST
REPUTATIONAL	Loss of Current Patients/Customers		$ 2,625,000	$ 3,274,000
	Loss of New Business		$ 225,000	
	Loss of Strategic Partners		$ 31,500	
	Loss of Staff		$ 392,500	
FINANCIAL	Remediation	Detection/Escalation Cost	$ 200,000	$ 2,517,560
		Credit & ID Theft Monitoring	$ 1,320,000	
		Mitigation Costs	$ 113,240	
		Lost Productivity	$ 300,000	
	Notification	Customer Notification	$ 229,000	
		Media Notification	$ 60,360	
		Attorney Fees	$ 69,960	
	Cyber Liability Insurance	New Policy or Deductible	$ 225,000	
	Change in Vendor (if BA-related)	RFP and Other Transition Costs	$ -	
LEGAL/REGULATORY	OCR Fines, Penalties and CAPs	Civil Monetary Penalty or Settlement	$ -	$ 2,594,495
		OCR Corrective Action Plan	$ 575,250	
	State Fines & Penalties	State Fines	$ 95,000	
		OCR Corrective Action Plan	$ 25,000	
	Class-Action Lawsuit	Settlement Costs	$ 1,363,396	
		Attorney Fees	$ 235,849	
		Insurance Dedcutible	$ 300,000	
OPERATIONAL	Cost of Hiring Additional IS Staff	Cost of New Hires	$ 375,000	$ 412,500
		Recruiting & Training Fees	$ 37,500	
	Cost of Reorganization		$ -	
CLINICAL	Fraudulent Claims Processed		$ 375,000	$ 375,000
	Delayed or Inaccurate Diagnosis		$ -	
GRAND TOTAL COST OF DATA BREACH				**$ 9,173,555**
% OF TOTAL ANNUAL REVENUE				**3.7%**
IMPACT				**MODERATE**
COST/RECORD				**$ 917**

Total Impact Scoring	
Insignificant	<2% of Revenue
Minor	2% of Revenue
Moderate	4% of Revenue
Major	6% of Revenue
Severe	>6% of Revenue

This model is not a boilerplate spreadsheet that can be used universally. Rather, it is one example of applying the PHive method for a breach costing from the PHI Project Report, sponsored by ANSI, Shared Assessments and the Internet Security Alliance in addtion to Clearwater Compliance and others, and developed for the specific scenario described in the report. Organizations will need to identify their own cost categories and customized spreadsheet depending upon their situation.

= "new" information

			high	medium	low	
Annual Revenues	$ 250,000,000					
# of records breached	10,000		25,000	10,000	5,000	
Reputational Repercussions						https://www.ibm.com/downloads/cas/861MNWN2
Loss of Revenues and related Margin						https://www.cbronline.com/breaches/cost-of-a-data-breach-soars-20-revenue-hacking-goes-classic-corporate/
a Loss of Current Revenues:			high	medium	low	https://www.globalsign.com/en/blog/cost-of-a-data-breach-and-procrastination/
Annual Revenues	$250,000,000					https://www.theamegroup.com/security-breach/
Patient or member churn due to reputational harm	7.0%		10.0%	7.0%	3.3%	https://www.ibm.com/downloads/cas/ZYKLN2E3
Loss of Current Revenues	$ 17,500,000					https://www.information-age.com/data-breaches-financial-impact-123470254/
b Loss of New Revenues:						https://www.securitymetrics.com/blog/how-much-does-data-breach-cost-your-organization
Forecast $ of new revenues next year	$15,000,000	$	50,000,000	$ 15,000,000	$ 8,000,000	
% new revenue loss due to negative publicity	10.0%		15.0%	10.0%	5.0%	
Loss of Forecast New Revenues	$ 1,500,000					
c Loss of Revenues from Strategic Partners:						
Forecast $ of new revenues next year	$3,000,000	$	8,000,000	$ 3,000,000	$ 1,000,000	company specific
% new revenue loss due to negative publicity	7.0%		10.0%	7.0%	3.3%	see reference above
Loss of Revenues from Strategic Partners	$ 210,000					
d Total Estimated Loss of Annual Revenues	$ 19,210,000					
% Variable Margin associated with Revenues	15.0%		7.0%	5.0%	3.0%	company specific
Total Estimated Loss of Margin due to Revenue Loss	$ 2,881,500					
						position-specific
Cost of Replacing Staff Leaving due to Reputational Damage:						https://www.norcal-group.com/library/71-of-cybersecurity-incidents-in-healthcare-involve-employee-actions
# of Staff Turnover	10					
Average Annual Salary	$ 125,000	$	200,000	$ 125,000	$ 50,000	https://www.recruiter.com/salaries/healthcare-professionals-salary.html
Recruiting Cost-Per-Hire (excludes advertising, travel, relocation)	30%		35%	30%	25%	http://www.businessknowhow.com/QandA/recruit.htm
Recruiting Cost of Replacing Staff	$ 375,000					
						# of days to fill a position
# of Days Lost Margin due to New Staff Search and Training	35		40	35	30	https://www.shrm.org/hr-today/trends-and-forecasting/research-and-surveys/Documents/2017-Talent-Acquisition-Benchmarking.pdf
Average Gross Margin per Staff per Day	$ 500		$750	$500	$250	company specific
Lost of Gross Margin due to New Staff Search	$ 17,500					
Total Estimated Cost or Margin due to Loss of Staff	$ 392,500					
Total Reputation Repercussions	$ 3,274,000					
	1.31%	of Annual Revenues				
Financial Repercussions						
Cost of Remediation			high	medium	low	https://www.winston.com/en/privacy-law-corner/costs-of-a-data-breach.html
a Detection/Escalation Cost: (forensic-investigation-assessment-audit-crisis management)						
# of records breached	10,000					https://www.secureworks.com/blog/data-breach-response-planning-cyber-threat-intelligence
Detection/Escalation Cost per record	$ 20.00	$	25.00	$ 20.00	$ 15.00	https://www.businessinsider.com/sc/data-breaches-cost-us-businesses-7-million-2017-4
Cost of Detection/Escalation	$ 200,000					
b1 Credit and Identity Theft Monitoring						
# of records breached	10,000					https://www.experian.com/blogs/ask-experian/identity-theft-statistics/
Cost of ID Theft and Credit Monitoring per month	$ 27.50	$	25.00	$ 27.50	$ 10.00	http://www.nextadvisor.com/identity_theft_protection_services/compare.php
# of Months Provided	24		24	18	12	company specific
% of victims taking advantage of Id Theft and Credit Monitoring	20%		25%	20%	15%	industry experts
Cost of Credit & ID Theft Monitoring	$ 1,320,000					
OR						
b2 Cost of Identity Theft						
# of records breached	10,000					
% of Records Exploited	25%		30%	25%	20%	https://www.lifelock.com/learn-identity-theft-resources-how-common-is-identity-theft.html
# of Victims	2,500					https://www.javelinstrategy.com/press-release/identity-fraud-hits-all-time-high-167-million-us-victims-2017-according-new-javelin
Average cost per victim	$ 500	$	1,000	$ 500	$ 250	
Total Cost of Identity Theft	$ -					
c Cost of Mitigation (internally determined)						
(1) Cost of Encryption						
# of laptops to be encrypted	50		100	50	5	incident specific
cost/month/laptop	$ 155	$	15.00	$ 12.95	$ 10.00	https://blog.primefactors.com/encryption-cost-protection-rpi
Cost of Encrypting Laptops	$ 93,240					https://www.howtogeek.com/347730/why-does-microsoft-charge-100-for-encryption-when-everyone-else-gives-it-away/
(2) Cost of replacing lost or stolen asset	$ 10,000	$	20,000	$ 10,000	$ 5,000	incident specific
(3) Cost of Workforce Retraining						
Number of Staff Requiring Retraining	200		100	50	25	incident specific
Required # Hours for Training	1.00		1.25	1.00	0.50	company specific
Average Hourly Pay per Trainee	### ################	$	65.00	$ 50.00	$ 37.50	https://www.hipaatraining.com/
Cost of Workforce Retraining	$ 10,000					
Total Cost of Mitigation (internally determined)	$ 113,240					
d Cost of Lost Productivity						
# of Records Breached	###### ##############					
Cost of Loss Productivity due to a Breach	$ 30.00	$	45.00	$ 30.00	$ 15.00	https://www.businessinsider.com/sc/data-breaches-cost-us-businesses-7-million-2017-4
Total Cost of Lost Productivity	$ 300,000					https://phoenixnap.com/blog/business-deterioration-after-a-data-breach
Total Cost of Remediation	$ 1,933,240					
Cost of Notification			high	medium	low	
# of records breached	10,000					
a Customer Notification						
per record cost of notification	$ 13.90	$	15.26	$ 13.90	$ 10.18	http://federalnewsnetwork.com/wp-content/uploads/2017/03/Best-Practices-for-Data-Breach-Notification-1.19.17_FINAL-DRAFT.pdf
per record cost of call center support	$ 9.00	$	10.80	$ 9.00	$ 7.20	
Total Notification Cost to Affected Individuals	$ 229,000					
b Notification to Media						
per record cost of Crisis Management Consulting	$ 5.04	$	6.05	$ 5.04	$ 4.03	
per record cost of Media Management	$ 1.00	$	1.20	$ 1.00	$ 0.80	
Total NotificationCosts to Media	$ 60,360					
c Attorney Fees for reviewing communications						
per record cost of Attorney's Fees	$ 7.00	$	8.40	$ 7.00	$ 56.00	

Total Attorney Fees	$ 69,960					
Total Cost of Notification	$ 359,320					
Cost of Cyber Liability Insurance (new policy or deductible)						
a Premium	$ 200,000	$ 225,000	$ 200,000	$ 175,000	company specific - check your policyu	
b Broker Fees	$ 25,000	15%	12.5%	10%	company specific - check your policy	
Total Cost of Cyber Liability Insurance (if new)	$ 225,000					
OR						
Cyber Liability Insurance Deductible	$ 375,000	$ 500,000	$ 375,000	$ 250,000	company specific - check your policy	
Deductible of Cost of Notification	$ -	company specific to coverage if carrying cyber liability insurance				
Cost of Changing Business Associate (if applicable)						
a Cost of Time on RFP and Due Diligence on New Vendor	$ -	as applicable, company specific				
b Cost of Transition to new BA						
# of months of transition	# ################					
Duplicated Cost per Month	# ################					
Duplicate Cost during Transition to New Vendor	$ -					
c Incremental Higher Annual Cost of New Vendor	$ -					
Total Cost of Changing Business Associate	$ -					
Total Financial Repercussions	$ 2,517,560					
	1.01%	of Annual Revenues				

Legal & Regulatory Repercussions

CASE EXAMPLES ORGANIZED BY ISSUE - OCR

Cost of OCR Fines, Penalties and CAP costs

for more information on the cost of your highest risks, click on url above

a1 Civil Monetary Penalty		willful neglect	willful neglect	reasonable		
Cause		uncorrected	corrected	cause	MD Anderson	http://www.shrm.org/research/benchmarks/documents/cost-per-hire%20article_final.pdf
Civil monetary penalty (rarely used)	$ -	$ 4,300,000	$ 3,200,000	$ 239,800	Children's Medical Center	http://www.nasrecruitment.com/docs/recruitment_hotsheets/Healthcare-Recruitment-Metrics.pdf
OR					Lincare	
a2 Settlement with OCR		faillure to	unauthorized	accessible		
Cause		detect hackers	disclosure	on internet	Anthem	
Settlement		$ 16,000,000	$ 2,200,000	$ 2,140,000	NY Presbyterian Hospital	
Settlement with OCR	$ -				St Joseph Hospital	
b Cost of OCR Corrective Action Plan						
(1) Develop and document updated/new Policies & Procedures	$ 15,000	$ 20,000	$ 15,000	$ 10,000	https://www.bizmanualz.com/leverage-technology/what-are-the-costs-of-managing-policies-and-procedures.html	
(2) Develop updated training for workforce	$ 10,000	$ 15,000	$ 10,000	$ 8,000	dependent on paper vs electronic, # of P&Ps, # of employees	
(3) Implement New Procedures and Train Workforce						93600
% of hour required for training	50%	100%	50%	25%	dependent on paper vs electronic, # of P&Ps, # of employees	
Average Hourly Wage	$ 40	#	### ##########	### #########	dependent on paper vs electronic, # of P&Ps, # of employees	
# of Workforce Members requiring Training	2,500	#	##### ##########	##### ########	dependent on paper vs electronic, # of P&Ps, # of employees	
Cost of Training Workforce (loss of productivity)	$ 50,000					
(4) # of new Staff Hired as needed to comply with Corrective Action Plan	2	3	2	1	# and salary dependent on company specifics	
Average Salary + Benefits per New Hire	$ 88,200	$ 132,300	$ 88,200	$ 44,100	https://www.recruiter.com/salaries/healthcare-professionals-salary.html	
% of Salary Recruiting Cost	25%	35%	25%	20%	http://www.businessknowhow.com/QandA/recruit.htm	
Cost of New Hires	$ 110,250					
(5) Implement New Safeguards	$ 200,000	$ 300,000	$ 200,000	$ 100,000	vulnerability specific-research solutions for your greatest risks	
(6) Conduct a Risk Analysis	$ 150,000	$ 200,000	$ 150,000	$ 100,000	dependent on size, # of locations, # of assets (Clearwater algorithm?)	
(7) Hire Independent Monitor and Annual reports on progress	$ 50,000	$ 75,000	$ 50,000	$ 25,000		
Total Cost of OCR Corrective Action Plan	$ 575,250					
Total OCR Fines, Penalties and CAP costs	$ 575,250					

Enter the total number of affected records here (no commas ie., 25000): 10000

	-20%	Average Cost	+20%
Internal Investigation			
Cybercrime consulting	55200	69000	82800
Attorney fees	55968	69960	83952
Sum:	$ 111168	$ 138960	$ 166752
Notification/Crisis Management			
Customer notification (certified mail)	101760	127200	152640
Call center support	72000	90000	108000
Crisis management consulting	40320	50400	60480
Media management	7968	9960	11952
Sum:	$ 222048	$ 277560	$ 333072
Regulatory/Compliance			
Credit monitoring for affected customers	462720	578400	694080
Regulatory investigation defense	171168	213960	256752
State/Federal fines or fees	363072	453840	544608
Sum:	$ 996960	$ 1246200	$ 1495440

State Fines and Penalties

a Fines					
Total State Fines	$ 95,000	$ 250,000	$ 95,000	$ 15,000	see "Examples of State Fines"
b Cost of State Corrective Action Plan (additional reporting requirements)	$ 25,000	$ 50,000	$ 25,000	$ 10,000	state specific- research the states where your patients/customers live
Total State Fines & Penalties	$ 120,000				

Class-Action Lawsuit

a Settlement Costs		Aetna	St Joseph	Anthem	
# of Breached Records	10,000	11,875	31,800	78,800,000	
Settlement payment per victim	$ 242	$ 500.00	$ 242.00	$ 0.20	see "Lawsuit Costs"
Total settlement payments for all victims	2,420,000				
% of breached records resulting in harm	0.38%	0.40%	0.38%	0.38%	see "Lawsuit Costs"
# of assumed harmed victims	38	47	120	300,000	
Payment per harmed victim	$ 25,000	$ 50,000	$ 25,000	$ 2,500	
Total settlement payments for harmed victims	$ 943,396				
Subtotal Settlement Costs to Victims	$ 3,363,396				
$ Covered by Insurance	$ 2,000,000	$ 2,000,000	$ 4,000,000	$ 8,000,000	see "Cyber Liability Insurance"
Company Settlement Costs to Victims	$ 1,363,396				company specific- check your cyber insurance policy
b Settlement Paid for Legal Support as a % paid for all Victims	$ 236	$ 4,300,000	$ 7,500,000	$ 31,050,000	see "Lawsuit Costs"
Legal Costs	$ 2,358,491				
% Covered by Insurance	90%	80%	90%	100%	company specific- check your insurance policy
Company Settlement Costs to Attorneys of Victims	$ 235,849				
c Insurance Deductible	$ 300,000	$ 500,000	$ 300,000	$ 100,000	company specific- check your insurance policy
d Consulting Firm or 3rd Party Administrator	$ -	$ 180,000	$ -	$ 23,000,000	company specific- check your insurance policy
Total Lawsuit Costs	$ 1,899,245				
Total Legal and Regulatory Repercussions	$ 2,594,495				
	1.04%	% of Annual Revenues			

Operational Repercussions

Cost of Hiring Additional Staff (not included in CAP)

a Additional Staff needed to Improved Security/Privacy (not included in CAP)					https://blackbookmarketresearch.newswire.com/news/84-of-healthcare-organizations-dont-have-a-cybersecurity-leader-as-the-20110145
Number of Staff Needed	5	10	5	2	incident specific
Average Annual Salary + Benefits per New Staff Member	$ 75,000	$ 90,000	$ 75,000	$ 60,000	company specific
Incremental Cost of New Hires	$ 375,000				
b Cost of Recruiting and Training new Hires					
Average Cost of Recruiting and Training per New Staff Member	$ 7,500	$ 10,000	$ 7,500	$ 5,000	company specific
Total Cost of Recruiting & Training New Hires	$ 37,500				
Total Cost of Hiring Additional Staff (not included in CAP or mitigation plan)	$ 412,500				
Cost of Reorganization	$ -				company specific
Total Operational Repercussions	$ 412,500				
	0.17%	% of Annual Revenues			

Clinical Repercussions

Fraudulent Claims Processed/Medical Identity Theft

# of Breached Records	10,000				http://www.medidfraud.org/2014-fifth-annual-study-on-medical-identity-theft/
% that result in Medical Fraudulent Claims Processed	1.0%				
# of Medical Fraudulent Claims Processed	50				
Average cost per claim	$7,500	$ 25,000	$ 13,500	$ 2,500	

Total Cost of Fraudulent Medical Claims Processed	$	375,000				
Delayed or Inaccurate Diagnosis						
% that result in Delayed or Inaccurate Diagnosis		3.0%	5%	3%	1%	
# of Delayed or Inaccurate Diagnosis		300				https://digitalguardian.com/blog/researcher-hospital-data-breaches-connected-patient-deaths
Average cost per claim						
Delayed or Inaccurate Diagnosis	$	-				
Total Clincial Repercussions	$	375,000	line 105 + line 106			
		0.15%	% of Annual Revenues			
Total Impact of Data Breach	**$**	**9,173,555**	line 17 + line 76 + line 96 + line 100 + line 107			
		3.7%	% of revenue			
		$917	average cost/record			

	Ponemon	Including Other Considerations
# of records breached	10,000	10,000
Average cost/record	$ 408	$ 917
Cost of a Breach	**$ 4,080,000**	**$ 9,173,555**
Probabilized # of years between breaches	2	2
Average annual cost of a probable breach	**$ 2,040,000**	**$ 4,586,778**
# of years between breaches	3	3
Annual cost of a breach	**$ 1,360,000**	**$ 3,057,852**
Annual $ investment with breakeven ROI	$ 680,000	$ 1,528,926
Probability of a Breach	29%	29%
Cost of a Breach (Probability Adjusted)	**$ 1,183,200**	**$ 2,660,331**
	2	2
Average annual cost of a probable breach	$ 591,600	$ 1,330,166
	5	5
Average annual cost of a probable breach	$ 236,640	$ 532,066
Annual $ investment with breakeven ROI	$ 354,960	$ 798,099

“On average, the breached firms lost 2.1 percent of their market value within two daysfollowing the public announcement.” What would you invest to protect your company's

Source: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html

Note: NY Presb and Columbia are combined together in the OCR list on HHS.gov website

	Cottage Health	Cottage Health Settles Potential Violations of HIPAA Rules for $3 Million
1	Pagosa Springs Medical Center	Colorado hospital failed to terminate former employee's access to electronic protected health information
2	Advanced Care Hospitalists	Florida contractor physicians' group shares protected health information with unknown vendor without a business associate agreement
3	Allergy Associates of Hartford	Allergy practice pays $125,000 to settle doctor's disclosure of patient information to a reporter
4	Anthem	Anthem Pays OCR $16 Million in Record HIPAA Settlement Following Largest U.S. Health Data Breach in History
5	Boston Medical Center	Unauthorized Disclosure of Patients' Protected Health Information During ABC Television Filming Results in Multiple HIPAA Settlements Totaling $999,000
6	Brigham and Women's Hospital	Unauthorized Disclosure of Patients' Protected Health Information During ABC Television Filming Results in Multiple HIPAA Settlements Totaling $999,000
7	Massachusetts General Hospital	Unauthorized Disclosure of Patients' Protected Health Information During ABC Television Filming Results in Multiple HIPAA Settlements Totaling $999,000
8	MD Anderson	Judge rules in favor of OCR and requires a Texas cancer center to pay $4.3 million in penalties for HIPAA violations
9	Filefax	Consequences for HIPAA violations don't stop when a business closes
10	Fresenius Medical Care North America	Five breaches add up to millions in settlement costs for entity that failed to heed HIPAA's risk analysis and risk management rules
11	#REF!	Failure to protect the health records of millions of persons costs entity millions of dollars
12	#REF!	Careless handling of HIV information jeopardizes patient's privacy, costs entity $387k
13	#REF!	Texas health system settles potential HIPAA disclosure violations
14	CardioNet	$2.5 million settlement shows that not understanding HIPAA requirements creates risk
15	Center for Children's Digestive Health	No Business Associate Agreement? $31K Mistake – April 20, 2017
16	Metro Communiity Provider Network	Overlooking risks leads to breach, $400,000 settlement
17	Memorial Healthcare Systems	$5.5 million HIPAA settlement shines light on the importance of audit controls
18	Children's Medical Center of Dallas	Lack of timely action risks security and costs money
19	MAPFRE Insurance	HIPAA settlement demonstrates importance of implementing safeguards for ePHI - January 18, 2017
20	Presence Health	First HIPAA enforcement action for lack of timely breach notification settles for $475,000 - January 9, 2017
21	University of Massachusetts Amherst (UMass)	UMass settles potential HIPAA violations following malware infection - November 22, 2016
22	St. Joseph Health (SJH)	$2.14 million HIPAA settlement underscores importance of managing security risk - October 17, 2016
23	Care New England Health System (CNE)	HIPAA settlement illustrates the importance of reviewing and updating, as necessary, business associate agreements - September 23, 2016
24	Advocate Health Care Network	Advocate Health Care Settles Potential HIPAA Penalties for $5.55 Million - August 4, 2016
25	University of Mississippi (UMMC)	Multiple alleged HIPAA violations result in $2.75 million settlement with the University of Mississippi Medical Center (UMMC) - July 21, 2016
26	Oregon Health & Science University (OHSU)	Widespread HIPAA vulnerabilities result in $2.7 million settlement with Oregon Health & Science University
27	Catholic Health Care Services (PHL)	Business Associate's Failure to Safeguard Nursing Home Residents' PHI Leads to $650,000 HIPAA Settlement – June 29, 2016
28	NY Presbyterian Hospital	Unauthorized Filming for "NY Med" Results in $2.2 Million Settlement with New York Presbyterian Hospital - April 21, 2016
29	Raleigh Orthopaedic Clinic, P.A.	$750,000 settlement highlights the need for HIPAA business associate agreements - April 16, 2016
30	The Feinstein Institute for Medical Research	Improper disclosure of research participants' protected health information results in $3.9 million HIPAA settlement - March 17, 2016
31	North Memorial Health Care of Minnesota	$1.55 million settlement underscores the importance of executing HIPAA business associate agreements - March 16, 2016
32	Complete P.T., Pool & Land Physical Therapy, Inc.	Physical therapy provider settles violations that it impermissibly disclosed patient information- February 16, 2016
33	Lincare, Inc.	Administrative Law Judge rules in favor of OCR enforcement, requiring Lincare, Inc. to pay $239,800 - February 3, 2016
34	University of Washington Medicine	$750,000 HIPAA Settlement Underscores the Need for Organization Wide Risk Analysis - December 14, 2015
35	Triple-S Management Corp.	Triple-S Management Corporation Settles HHS Charges by Agreeing to $3.5 Million HIPAA Settlement - November 30, 2015
36	Lahey Clinic Hospital	HIPAA Settlement Reinforces Lessons for Users of Medical Devices - November 24, 2015
37	Cancer Care Group, P.C.	$750,000 HIPAA Settlement Emphasizes the Importance of Risk Analysis and Device and Media Control Policies - August 31, 2015
38	St. Elizabeth's Medical Center	HIPAA Settlement Highlights Importance of Safeguards When Using Internet Applications - June 10, 2015
39	Cornell Prescription Pharmacy	HIPAA Settlement Highlights the Continuing Importance of Secure Disposal of Paper Medical Records - April 22, 2015
40	Anchorage Community Mental Health Services	HIPAA Settlement Underscores the Vulnerability of Unpatched and Unsupported Software - December 2, 2014
41	Parkview Health Systems, Inc.	$800,000 HIPAA Settlement in Medical Records Dumping Case - June 23, 2014
42	NY Presbyterian Hospital	Data Breach Results in $4.8 Million HIPAA Settlements - May 7, 2014
43	Columbia University Medical Center	Data Breach Results in $4.8 Million HIPAA Settlements - May 7, 2014
44	Concentra Health Services	Concentra Settles HIPAA Case for $1,725,220 - April 22, 2014
45	QCA Health Plan, Inc.	QCA Settles HIPAA Case for $250,000 – April 22, 2014
46	Skagit County, WA	County Government Settles Potential HIPAA Violations - March 7, 2014
47	AP Derm	Resolution Agreement with Adult & Pediatric Dermatology, P.C. of Massachusetts - December 20, 2013
48	Affinity Health Plan	HHS Settles with Health Plan in Photocopier Breach Case - August 14, 2013
49	WellPoint (Anthem)	WellPoint Settles HIPAA Security Case for $1,700,000 - July 11, 2013
50	Shasta Regional Medical Center	Shasta Regional Medical Center Settles HIPAA Privacy Case for $275,000 - June 13, 2013
51	Idaho State University	Idaho State University Settles HIPAA Security Case for $400,000 - May 21, 2013
52	Hospice of Northern Idaho	HHS announces first HIPAA breach settlement involving less than 500 patients - December 31, 2012
53	Massachusetts Eye and Ear	Massachusetts Provider Settles HIPAA Case for $1.5 Million – September 17, 2012
54	Alaksa DHSS	Alaska DHSS Settles HIPAA Security Case for $1,700,000 – June 26, 2012
55	Phoenix Cardiac Surgery	HHS Settles Case with Phoenix Cardiac Surgery for Lack of HIPAA Safeguards - April 13, 2012
56	BlueCross BlueShield of TN	HHS settles HIPAA case with BCBST for $1.5 million - March 13, 2012
57	UCLA	Resolution Agreement with the University of California at Los Angeles Health System - July 6, 2011
58	Mass General	Resolution Agreement with General Hospital Corp. & Massachusetts General Physicians Organization, Inc. - February 14, 2011
59	Cignet	Civil Money Penalty issued to Cignet Health of Prince George's County, MD - February 4, 2011
60	Mgmt Svcs Org of Washington	Resolution Agreement with Management Services Organization Washington, Inc. - December 13, 2010
61	Rite Aid	Resolution Agreement with Rite Aid Corporation - July 27, 2010
62	CVS	Resolution Agreement with CVS Pharmacy, Inc. - January 16, 2009
63	Providence Health	Resolution Agreement with Providence Health & Services - July 16, 2008

State Fines

California	Cottage Health Fined $2 Million By California Attorney General's Office	https://www.hipaajournal.com/cottage-health-fined-2-million-california-attorney-generals-office/
Connecticcut	A HOSPITAL AND ITS TECHNOLOGY PARTNER SHARE $90K HIPAA FINE	https://digitalguardian.com/blog/hospital-and-its-technology-partner-share-90k-hipaa-fine
Connecticut	Connecticut hospital and BA pay $90,000 fine for HIPAA violation	http://www.hcpro.com/HIM-322735-865/Connecticut-hospital-and-BA-pay-90000-fine-for-HIPAA-violation.html
Connecticut	Hartford Hospital, EMC Corp. Fined for HIPAA Violations	https://www.healthdatamanagement.com/news/hartford-hospital-emc-corp-fined-for-hipaa-violations
Illinois	Illinois AG sues records storage company FileFax for dumping thousands of Suburban Lung Associates' patients' records	https://www.databreaches.net/illinois-ag-sues-records-storage-company-filefax-for-dumping-thousands-of-suburban-lung-associates-patients-records/
Indiana	$1.44M HIPAA award upheld after Walgreen pharmacist shared patient data	https://www.indystar.com/story/news/2014/11/14/m-award-upheld-walgreen-pharmacist-shared-patient-data/19035783/
Massachusetts	SOUTH SHORE HOSPITAL TO PAY $750,000 TO SETTLE DATA BREACH CHARGES	https://www.healthleadersmedia.com/innovation/south-shore-hospital-pay-750000-settle-data-breach-charges
Minnesota	ACCRETIVE AGREES TO $2.5M FINE; COMPANY TO WITHDRAW FROM MN	https://www.healthleadersmedia.com/finance/accretive-agrees-25m-fine-company-withdraw-mn
Multi-State	12 State Attorneys General Unite in the First Multi-State Enforcement of Alleged HIPAA Privacy Breach	https://ankura.com/insights/12-state-attorneys-general-unite-in-the-first-multi-state-enforcement-of-alleged-hipaa-privacy-breach/
Multi-State	Aetna Reaches Settlements with State AGs Over HIPAA Violations	https://healthitsecurity.com/news/aetna-reaches-settlements-with-state-ags-over-hipaa-violations
New Jersey	NJ AG Smacks Practice With Hefty Fine for Vendor Breach	https://www.bankinfosecurity.com/nj-ag-smacks-practice-hefty-fine-for-vendor-breach-a-10774
New York State	State HIPAA Settlement Reached in URMC Data Breach Case	https://healthitsecurity.com/news/state-hipaa-settlement-reached-in-urmc-data-breach-case
New York State	A.G. Underwood Announces Settlement With EmblemHealth To Ensure Health Insurance Coverage For Gender Reassignment Surg	https://ag.ny.gov/press-release/ag-underwood-announces-settlement-emblemhealth-ensure-health-insurance-coverage-gender
Vermont	Vermont Attorney General Agrees $264,000 SAManage USA Data Breach Settlement	https://www.hipaajournal.com/samanage-usa-data-breach-settlement/

	Paid to Victims	# of Victims	Paid per Victim	Credit Monitoring	Legal Fees	Consulting Firm/Administrator	ID Theft or Harm	Paid per Victim	# of Victims Assume	% of Total Victims	Total Cost Before Remediation	
Aetna	$ 5,937,500	11,875	$ 500.00	$ 1,500,000	$ 4,300,000	$ 180,000	$ 943,700	$ 20,000	47	0.40%	$ 12,861,200	https://khn.org/news/its-in-the-mail-aetna-agrees-to-17m-payout-in-hiv-privacy-breach/
St Joseph Health	$ 7,500,000	31,800	$ 242.00	$ 4,500,000	$ 7,500,000		$ 3,000,000	$ 25,000	120	0.38%	$ 22,500,000	https://www.beckershospitalreview.com/payer-issues/aetna-to-pay-4-3m-in-attorney-fees-related-to-hiv-privacy-breach.html
Anthem	$ 15,950,000	78,800,000	$ 0.20	$ 30,000,000	$ 31,050,000	$ 23,000,000	$ 15,000,000	$ 50	300,000	0.38%	$ 115,000,000	https://healthpayerintelligence.com/news/aetna-agrees-to-17m-settlement-in-hiv-privacy-data-breach
												https://www.hipaajournal.com/st-joseph-health-settles-class-action-data-breach-lawsuit-3354/
												https://www.healthleadersmedia.com/anthem-agrees-record-setting-class-action-settlement-2015-breach
												https://www.bankinfosecurity.com/judge-gives-final-approval-to-115m-anthem-settlement-a-11399
												https://www.huntonprivacyblog.com/2018/08/24/judge-grants-final-approval-record-data-breach-settlement-anthem-class-action/

Cyber Liability Insurance - Common Coverage

http://www.reuters.com/article/us-cybersecurity-insurance-insight-idUSKCN0S609M20151012

- Cyber insurance very focused on healthcare—significant competition between insurance companies
  - e.g. health care system 10,000 employees
    - $10MM limit
    - Deductible of $250,000 - $500,000
    - Premium $175,000/year - $225,000
- Coverage:
  - 3rd party liability: $10MM with sub-limits of $2MM for breach response and $250K for defense costs
  - Breach response coverage: notification, crisis management (PR & law firm guidance), ID theft monitoring, forensics, fix-its, fines and penalties: credit card fines & penalties, government regulatory settlements (not fines and penalties), consumer redress

How the cost of a data breach is calculated

To calculate the cost of a data breach, we use an accounting methodology called activity-based costing (ABC). This methodology identifies activities and assigns a cost according to actual use. The ABC methodology is fully explained in Part 5 of this report.

Four process-related activities drive a range of expenditures associated with an organization's data breach detection, escalation, notification, and activities conducted following a data breach. The four cost centers are:

> Detection and escalation:

Activities that enable a company to detect and report the breach to appropriate personnel within a specified time period.

Examples:

- Forensic and investigative activities
- Assessment and audit services
- Crisis team management
- Communications to executive management and board of directors

> Notification costs:

Activities that enable the company to notify individuals who had data compromised in the breach (data subjects) as regulatory activities and communications.

Examples:

- Emails, letters, outbound telephone calls, or general notice that personal information was lost or stolen
- Communication with regulators; determination of all regulatory requirements, engagement of outside experts

> Post data breach response:

Processes set up to help individuals or customers affected by the breach to communicate with the company, as well as costs associated with redress activities and reparation with data subjects and regulators.

Examples:

- Help desk activities/inbound communications
- Credit report monitoring and identity protection services
- Issuing new accounts or credit cards
- Legal expenditures
- Product discounts
- Regulatory interventions (fines)

> Lost business cost:

Activities associated with cost of lost business including customer churn, business disruption, and system downtime.

Examples:

- Cost of business disruption and revenue losses from system downtime
- Cost of lost customers and acquiring new customers
- Reputation losses and diminished goodwill

https://www.ibm.com/downloads/cas/861MNWN2