United States Health and Human Services
"Resolution Agreements" Regarding HIPAA Violations
10.2016

	Covered Entity/ Year of Agreement	Breach	Deficiencies Found	Civil $ Penalties, notable terms
40	Care New England Health System – Mass. and RI 2016	Loss of unencrypted backup tapes of ultrasounds of 14,000 individuals; business associate agreement had not been updated to include current regulations.	Failure to provide security for backup tapes; failure to update business associate agreement with legal updates, failure to timely notify individuals of breach.	$400,000; separate consent judgment with Mass. Attorney General for $150,000
39	Advocate Health Care - Illinois 2016	E-PHI of 4 million individuals at risk from physical security gaps at data center leading to computer thefts; unencrypted laptop left in unlocked vehicle overnight, and unauthorized 3d party accessed PHI held by a business associate (3 separate breaches).	Many years of gaps in Security Rule protections, failure to do security risk analysis, failure to obtain business associate agreement before disclosing PHI;	$5.5 million
38	University of Mississippi Medical Center 2016	Password-protected laptop missing, likely stolen; generic username and passwords were allowed for access to network drive, so 10,000 individuals' PHI was at risk.	Lack of follow-up on known risks; physical security gaps; generic username and password were used.	$2.75 million
37	Oregon Health & Science University 2016	Unencrypted laptops and stolen unencrypted thumb drive; multiple breaches involving thousands of individuals' PHI.	Use of cloud-based server without a BA agreement; incomplete risk analysis and incomplete follow-up to identified issues.	$2.7 million
36	Catholic Health Services – Philadelphia 2016	Theft of an unencrypted mobile device, not password-protected, of a Business Associate of 6 nursing homes – 412 individuals' PHI.	Lack of policies on mobile devices or on incidents, no risk management plan or HIPAA risk analysis	$650,000
35	New York Presbyterian 2016	Disclosure of two patients' PHI to film crews and staff during the filming of "NY Med," an ABC television series, with no authorization from the patients.	Lack of basic safeguards for protected health information; blatant disregard for privacy.	$2.2 million

United States Health and Human Services
"Resolution Agreements" Regarding HIPAA Violations
10.2016

	Covered Entity/ Year of Agreement	Breach	Deficiencies Found	Civil $ Penalties, notable terms
34	Raleigh Orthopaedic Clinic, P.A. of North Carolina 2016	Release of x-ray films and other PHI of 17,300 patients to a contractor without first obtaining a business associate agreement.	Failure to obtain a business associate agreement prior to disclosure of PHI; lack of management of business associate procedures.	$750,000
33	Feinstein Institute for Medical Research, New York 2016	Laptop computer containing the electronic PHI of ~ 13,000 patients and research participants was stolen from an employee's car. PHI included names, SSNs, dates of birth, extensive medical information.	Failure to implement safeguards to restrict access to unauthorized users, lack of policies and procedures to govern the receipt and removal of laptops that contained ePHI into and out of its facilities.	$3.9 billion
32	North Memorial Health Care 2016	Unencrypted, password-protected laptop was stolen from a business associate's locked vehicle; 9,497 individuals' PHI.	Failure to implement a business associate agreement with a major contractor and failing to institute an organization-wide risk analysis	$1.55 million
31	Complete P.T., Pool & Land Physical Therapy, Inc., Los Angeles 2016	Posted patient testimonials, including full names and full face photos, to its website without obtaining valid, HIPAA-compliant authorizations	Failed to reasonably safeguard PHI	$25,000
30	Lincare, Inc. 2016	Abandonment of documents with PHI of 278 individuals in a different home care setting.	Lack of policies governing PHI that is moved off-site; practice of storing PHI in employee's cars; minimal corrective action taken.	Civil Money penalties imposed by OCR and upheld by ALJ $239,000

United States Health and Human Services
"Resolution Agreements" Regarding HIPAA Violations
10.2016

	Covered Entity/ Year of Agreement	Breach	Deficiencies Found	Civil $ Penalties, notable terms
29	The University of Washington Medicine (UWM) 2015	Electronic PHI of ~ 90,000 individuals was accessed after an employee downloaded an email attachment that contained malicious malware.	Failure to implement policies and procedures to prevent, detect, contain, and correct security violations in multiple environments of healthcare.	$750,000
28	Triple-S Management Corporation 2015	multiple breach notifications from TRIPLE-S involving unsecured protected health information (PHI),	Failure to implement appropriate administrative, physical, and technical safeguards	$3.5 million
27	Lahey Hospital and Medical Center (Lahey) 2015	a laptop was stolen from an unlocked treatment room during the overnight hours on August 11, 2011	Lack of risk analysis and failure to safeguard euipment	$850,000
26	Cancer Care Group, LLC 2015	Laptop and unencrypted backup media stolen from employee's car, including PHI of 55,000 current and former patients	-Lack of risk analysis -Lack of policies on electronic security	$750,000 Risk analysis, risk management plan
25	St. Elizabeth's Medical Center 2015	-An internet-based document sharing application was used to store documents containing electronic protected health information (ePHI) of at least 498 individuals without having analyzed the risks associated with such a practice, AND -ePHI stored on former employee's personal laptop and flash drive (595 individuals).	Failure to -timely identify the problem -respond -mitigate the harmful effects and -document the incident and its outcome.	$218,400
24	Cornell Prescription Pharmacy 2015	Disposal of unsecured documents containing the protected health information (PHI) of 1,610 patients in an unlocked, open container on the provider's premises.	Failure to implement any written policies and procedures as required by the HIPAA Privacy Rule	$125,000

United States Health and Human Services
"Resolution Agreements" Regarding HIPAA Violations
10.2016

	Covered Entity/ Year of Agreement	Breach	Deficiencies Found	Civil $ Penalties, notable terms
23	Anchorage Community Mental Health Services (ACMHS) 2014	Malware compromising the security of information technology resources resulted in a breach of unsecured electronic protected health information (ePHI) affecting 2,743 individuals,	Un-patched and un-supported software, failure to follow own policies	$150,000
22	Parkview Health System 2014	71 boxes (~5,000-8,000 patients) of medical records delivered to public site known to be unattended.	-failure to safeguard non-electronic PHI	$800,000
21	New York and Presbyterian Hospital AND Columbia University 2014	6,800 individuals' ePHI disclosed. Deactivation of a personally-owned server on shared network made ePHI available on internet search engines.	-Neither entity had assured security of server -Neither had assured software protections -Neither had done Risk Assessment -NYP lacked P&Ps on database access, and failed to comply with other IT policies	$4,800,000 _____ NYP $3,300,000 CU $1,500,000
20	Concentra Health Services 2014	Laptop stolen from facility (# of individuals not shown in online reports)	-Incomplete and inconsistent efforts to encrypt devices -Insufficient security management processes	$1,725,220
19	QCA Health Services 2014	Laptop stolen from employee's car (148 individuals' PHI)	-Devices unencrypted -Multiple noncompliance issues	$250,000
18	Skagit County, WA 2014	ePHI of 1,581 individuals inadvertently publicly available internet on a publicly accessible server	-General and widespread noncompliance with privacy and security rules	$215,000

United States Health and Human Services
"Resolution Agreements" Regarding HIPAA Violations
10.2016

	Covered Entity/ Year of Agreement	Breach	Deficiencies Found	Civil $ Penalties, notable terms
17	Adult & Pediatric Dermatology, PC. 2013	Unencrypted thumb drive stolen from Ee's vehicle (2,200 individuals' PHI)	-no P&Ps in place re: breach notification -no analysis of risk to ePHI as part of security management process	$150,000 Risk analysis and risk mgmt. plans required.
16	Affinity Health Plan, New York 2013	Photocopier hard drive sold to CBS Evening News without PHI erased. (est. 344,579 individuals)	-ePHI not included in risk analysis -no P&P governing return of copiers to leasing agents	$1,215,780 15 facilities under same ownership required to attest to understanding of HIPAA.
15	WellPoint, Inc. managed care 2013	Online application database accessible to unauthorized persons over Internet. (612,402 individuals' names, DOB, SSNs, phone numbers, health info.)	-no technical evaluation of software upgrade to information systems -inadequate P&P implementation on authorizing access -no technical safeguards to verify those seeking access	$1.7 million
14	Shasta Regional Med. Ctr., California 2013	Two senior staff met with media to discuss medical services provided to an individual, and e-mail to all workforce re: the individual's condition.	-intentional disclosure to multiple media, multiple occasions -failure to sanction staff	$275,000
13	Idaho State University 2013	Disabled firewall protections left ePHI unsecured for 10 months. (17,500 individuals)	-inadequate security measures -no routine review of IT system	$400,000
12	Hospice of North Idaho 2012	Unencrypted laptop containing PHI was stolen (441 individuals)	-no risk analysis -no policies re: mobile device security	$50,000

United States Health and Human Services
"Resolution Agreements" Regarding HIPAA Violations
10.2016

	Covered Entity/ Year of Agreement	Breach	Deficiencies Found	Civil $ Penalties, notable terms
11	Massachusetts Eye & Ear Infirmary 2012	Theft of unencrypted personal laptop containing PHI (prescriptions, clinical info)	-no risk analysis re: portable devices -no security measures re: portable devices -P&Ps -extended period of time	$1.5 million
10	Alaska DHHS 2012	USB hard drive "possibly" containing PHI stolen from employee's vehicle	-no risk analysis -no risk mgmt. measures -no security training -no device and media controls -no assessment of device and media encryption	$1.7 million
9	Phoenix Cardiac Surgery 2012	Posting clinical and surgical appointments on Internet-based calendar that was publicly accessible	-few P&Ps -limited safeguards for electronic PHI -multi-year failure	$100,000
8	BCBS of Tenn. 2012	57 unencrypted computer hard drives stolen from leased facility (over 1 million individuals, incl. SSNs)	-no safeguards -no security evaluation of location -no facility access controls	$1.5 million
7	UC Los Angeles Health System 2011	Employees repeatedly, w/o permissible reason, looked at electronic PHI of 2 celebrity patients and numerous others	-no restriction on access -no sanctions for violations	$865,500
6	Mass. General 2011	Employee left schedule of 192 patients on subway train	-no safeguards on info removed from premises	$1 million
5	Cignet Health, Md. 2011	Denied 41 patients access to their medical records. Refused to produce records or otherwise cooperate with OCR.	-Willful neglect ($3 M)	$4.3 million
4	MSO Washington, Inc. 2010	Disclosures to an entity owned by MSO, which used the PHI for marketing purposes. In conjunction with a False Claims Act case.	-P&P revisions needed -Impermissible disclosures	$35,000

United States Health and Human Services
"Resolution Agreements" Regarding HIPAA Violations
10.2016

	Covered Entity/ Year of Agreement	Breach	Deficiencies Found	Civil $ Penalties, notable terms
			-Administrative, physical and technical safeguards	
3	Rite Aid 2010	Disposal of PHI in industrial trash containers open to the public, in several cities nationwide	-P&Ps on safeguards during disposal of PHI -No training on disposal -No sanctions	$1 million
2	CVS, Inc. 2009	Disposal of PHI in dumpsters accessible by the public	-P&Ps on safeguards during disposal of PHI -No training on disposal -No sanctions	$2.25 million
1	Providence Health Svcs. 2008	Backup tapes, optical disks and laptops with unencrypted PHI removed from premises and then lost or stolen. 386,000 patients.	-P&P on technical safeguards re: offsite transport and storage of PHI -Training	$100,000

Source:
http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html