United States Health and Human Services
"Resolution Agreements" Regarding HIPAA Violations
1.2014

1	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.
2	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.
3	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
4	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
5	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
6	Hospice of North Idaho 2012	Unencrypted laptop containing PHI was stolen (441 individuals)	-no risk analysis -no policies re: mobile device security	$50,000
7	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
8	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
10	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
11	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
12	Mass. General 2011	Employee left schedule of 192 patients on subway train	-no safeguards on info removed from premises	$1 million
13	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
14	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 -Administrative, physical and technical safeguards	$35,000
15	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
16	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
17	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/ocr/privacy/hipaa/enforcement/examples/index.html