Cooley

Select HIPAA Privacy and Security Enforcement Actions

Current as of August 2016

SELECT HIPAA PRIVACY AND SECURITY ENFORCEMENT ACTIONS

Settling Party	Business Associate or Covered Entity	Enforcing Party	Alleged HIPAA Violation(s)	Date of Resolution	Resolution Imposed	Additional Information
Advocate Health Care System (Advocate)	Covered Entity	Office for Civil Rights	• Between August and November of 2013, Advocate submitted three breach notification reports pertaining to separate and distinct incidents involving its subsidiary, Advocate Medical Group ("AMG"). • The first incident involved the theft of four desktops from one of AMG's offices containing patient records. The second incident involved the breach of ePHI of AMG patient data by a subcontractor billing company. The third incident involved the theft of an unencrypted laptop from the car of an AMG employee containing patient files with ePHI. • The combined breaches affected the ePHI of	August 8, 2016	• $5.55 million in civil monetary penalties. • 2 year corrective action plan which includes: modifying the existing risk analysis; developing and implementing a risk management plan; implement a process for evaluating environmental and operational changes; review and revise policies and procedures on device and media controls; review and revise policies and procedures on facility access controls; review and revise policies and	• This is the largest HIPAA settlement amount to date.

This chart summarizes certain information related to select public government settlements. It is based solely on public sources and is not an exhaustive list of HIPAA privacy and security enforcement actions.

SELECT HIPAA PRIVACY AND SECURITY ENFORCEMENT ACTIONS

Settling Party	Business Associate or Covered Entity	Enforcing Party	Alleged HIPAA Violation(s)	Date of Resolution	Resolution Imposed	Additional Information

			approximately 4 million individuals. The ePHI included demographic information, clinical information, health insurance information, patient names, addresses, credit card numbers and their expiration dates, and dates of birth.
			• OCR's investigations into these incidents revealed that Advocate failed to:
			  • conduct an accurate and thorough assessment of the potential risks and vulnerabilities to all of its ePHI;
			  • implement policies and procedures and facility access controls to limit physical access to the electronic information systems
					procedures related to business associates; develop an enhanced privacy and security awareness training program.
					• In addition to the above, Advocate must designate a contact person to overview and coordinate with HHS on the written plan of remediation and engage an independent assessor to determine if Advocate is complying with the remediation plan.	

This chart summarizes certain information related to select public government settlements. It is based solely on public sources and is not an exhaustive list of HIPAA privacy and security enforcement actions.

SELECT HIPAA PRIVACY AND SECURITY ENFORCEMENT ACTIONS

Settling Party	Business Associate or Covered Entity	Enforcing Party	Alleged HIPAA Violation(s)	Date of Resolution	Resolution Imposed	Additional Information
			housed within a large data support center; • obtain satisfactory assurances in the form of a written business associate contract that its business associate would appropriately safeguard all ePHI in its possession; and • reasonably safeguard an unencrypted laptop when left in an unlocked vehicle overnight.			
University of Mississippi Medical Center (UMMC)	Covered Entity	Office for Civil Rights	• On March 21, 2013, OCR was notified of a breach, after UMMC's privacy officer discovered that a password-protected laptop was missing from UMMC. UMMC's investigation concluded that it had likely been stolen by a visitor to the MICU who had	July 25, 2016	• $2,700,500 in civil monetary penalties. • 3 year corrective action plan, which includes: designation of an internal monitor; development of a monitor plan;	

This chart summarizes certain information related to select public government settlements. It is based solely on public sources and is not an exhaustive list of HIPAA privacy and security enforcement actions.

SELECT HIPAA PRIVACY AND SECURITY ENFORCEMENT ACTIONS

Settling Party	Business Associate or Covered Entity	Enforcing Party	Alleged HIPAA Violation(s)	Date of Resolution	Resolution Imposed	Additional Information
			inquired about borrowing one of the laptops. OCR's investigation revealed that ePHI stored on a UMMC network drive was vulnerable to unauthorized access via UMMC's wireless network, because users could access an active directory containing 67,000 files after entering a generic username and password. The directory included 328 files containing the ePHI of an estimated 10,000 patients dating back to 2008. • UMMC failed to implement appropriate policies and procedures to prevent, detect, contain, and correct security violations. • UMMC failed to implement physical safeguards for all workstations.		retention of records for monitoring; validation review to ensure monitoring plan is implemented and followed; drafting of an enterprise-wide risk analysis and risk management plan with approval from HHS; update Information Security Policies and any other necessary security policies; revision of breach notification policies with approval from HHS; development and implementation of a plan to provide unique name and/or number identifying and tracking users;	

This chart summarizes certain information related to select public government settlements. It is based solely on public sources and is not an exhaustive list of HIPAA privacy and security enforcement actions.

SELECT HIPAA PRIVACY AND SECURITY ENFORCEMENT ACTIONS

Settling Party	Business Associate or Covered Entity	Enforcing Party	Alleged HIPAA Violation(s)	Date of Resolution	Resolution Imposed	Additional Information
			• UMMC failed to assign a unique user name and/or number for identifying and tracking user identity. • UMMC failed to notify all individuals of the breach of PHI.		security awareness and training.	
Oregon Health & Science University (OHSU)	Covered Entity	Office for Civil Rights	• OHSU submitted multiple breach reports affecting thousands of individuals, including two reports involving unencrypted laptops and another large breach involving a stolen unencrypted thumb drive. • OCR investigation uncovered evidence of widespread vulnerabilities within OHSU's HIPAA compliance program, including the storage of the electronic PHI of over 3,000 individuals on a cloud-based server without a	July 18, 2016	• $2,700,000 in civil monetary penalties. • 3 year corrective action plan. Requires OHSU: Conduct an accurate assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI; develop a comprehensive risk management plan; provide risk analysis and risk management plan to HHS for	• OHSU performed risk analyses in 2003, 2005, 2006, 2008, 2010, and 2013, but OCR's investigation found that these analyses did not cover all ePHI in OHSU's enterprise, as required by the Security Rule. While the analyses identified vulnerabilities and risks to ePHI located in many areas of the organization, OHSU did not act in a timely manner to implement

This chart summarizes certain information related to select public government settlements. It is based solely on public sources and is not an exhaustive list of HIPAA privacy and security enforcement actions.

SELECT HIPAA PRIVACY AND SECURITY ENFORCEMENT ACTIONS

Settling Party	Business Associate or Covered Entity	Enforcing Party	Alleged HIPAA Violation(s)	Date of Resolution	Resolution Imposed	Additional Information
			BAA. • OHSU failed to implement policies and procedures to prevent, detect, contain, and correct security violations. • OHSU failed to implement a mechanism to encrypt and decrypt ePHI or an equivalent alternative measure for all ePHI maintained in OHSU's enterprise.		approval; provide HHS with an update regarding encryption status which shall include plan to manage personally-owned and OHSU owned devices and USBs; conduct security awareness training.	measures to address these documented risks and vulnerabilities to a reasonable and appropriate level. OHSU also lacked policies and procedures to prevent, detect, contain, and correct security violations and failed to implement a mechanism to encrypt and decrypt ePHI or an equivalent alternative measure for ePHI maintained on its workstations, despite having identified this lack of encryption as a risk
Catholic Health Care Services of the	Business Associate	Office for Civil Right	• Received breach notifications from each of the six nursing homes	June 24, 2016	• $650,000 in civil monetary penalties • 2 year corrective	• First settlement of HIPAA claims against a business associate

This chart summarizes certain information related to select public government settlements. It is based solely on public sources and is not an exhaustive list of HIPAA privacy and security enforcement actions.

SELECT HIPAA PRIVACY AND SECURITY ENFORCEMENT ACTIONS

Settling Party	Business Associate or Covered Entity	Enforcing Party	Alleged HIPAA Violation(s)	Date of Resolution	Resolution Imposed	Additional Information
Archdiocese of Philadelphia (CHCS)			which CHCS is the parent and which CHCS provides management services to • OCR found CHCS failed to conduct an accurate and through assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of e-PHI held by CHCS • OCR found CHCS failed to implement appropriate security measures to reduce the risks and vulnerabilities to a reasonable and appropriate level to comply with the Security Rule		action plan requires CHCS to conduct a risk assessment and document security measures implemented (or being implemented); develop Security Rule policies and procedures and provide for review to HHS; and shall distribute all updated policies to workforce members	
New York Presbyterian Hospital	Covered Entity	Office for Civil Rights	• Disclosure of two patients' PHI to film crews and staff during the filming of NY Med, an ABC television series, without first obtaining authorization	April 19, 2016	• $2.2 million in civil monetary penalties • 2 year corrective action plan requires NYP to revise HIPAA	• OCR also found that NYP failed to safeguard protected health information and allowed ABC film crews virtually unfettered

This chart summarizes certain information related to select public government settlements. It is based solely on public sources and is not an exhaustive list of HIPAA privacy and security enforcement actions.

SELECT HIPAA PRIVACY AND SECURITY ENFORCEMENT ACTIONS

Settling Party	Business Associate or Covered Entity	Enforcing Party	Alleged HIPAA Violation(s)	Date of Resolution	Resolution Imposed	Additional Information
			from patients. • OCR found that NYP allowed the ABC crew to film someone who was dying and another person in significant distress, even after a medical professional urged the crew to stop		policies and procedures and submit to OCR for review; policies and procedures will be distributed to all workforce members; and training for all employees on those policies and procedures shall occur.	access to its health care facility, effectively creating an environment where PHI could not be protected from impermissible disclosure to the ABC film crew and staff.
Raleigh Orthopaedic Clinic P.A. of North Carolina	Covered Entity	Office for Civil Rights	• Raleigh handed over PHI for approximately 17,300 patients to a potential business partner without first executing a business associate agreement. • The business partner promised to transfer x-ray film and related PHI to electronic media in exchange for harvesting the silver from the x-ray films	April 14, 2016	• $750,000 in civil monetary penalties • 2 year corrective plan, Raleigh will provide OCR with an inventory of all contracts and business associate agreements and copies of all those business associate agreements; revise policies and	

This chart summarizes certain information related to select public government settlements. It is based solely on public sources and is not an exhaustive list of HIPAA privacy and security enforcement actions.

SELECT HIPAA PRIVACY AND SECURITY ENFORCEMENT ACTIONS

Settling Party	Business Associate or Covered Entity	Enforcing Party	Alleged HIPAA Violation(s)	Date of Resolution	Resolution Imposed	Additional Information
					procedures to designate a person responsible for business associate agreement execution and policies and procedures defining when business associate agreements are necessary; establish a process for assessing whether entities are business associates; designate a responsible individual to ensure business associate agreements are in place prior to disclosing PHI to a business associate; create a standard template business associate agreement; establish a standard	

This chart summarizes certain information related to select public government settlements. It is based solely on public sources and is not an exhaustive list of HIPAA privacy and security enforcement actions.

SELECT HIPAA PRIVACY AND SECURITY ENFORCEMENT ACTIONS

Settling Party	Business Associate or Covered Entity	Enforcing Party	Alleged HIPAA Violation(s)	Date of Resolution	Resolution Imposed	Additional Information
					process for maintaining documentation of a business associate agreements for at least six (6) years beyond the date of termination of a business associate relationship; and limit disclosures of PHI to any business associate to the minimum necessary to accomplish the purpose for which the business associate was hired, revised policies and procedures must be provided to OCR for review; training materials will also be revised to reflect business associate	

This chart summarizes certain information related to select public government settlements. It is based solely on public sources and is not an exhaustive list of HIPAA privacy and security enforcement actions.

SELECT HIPAA PRIVACY AND SECURITY ENFORCEMENT ACTIONS

Settling Party	Business Associate or Covered Entity	Enforcing Party	Alleged HIPAA Violation(s)	Date of Resolution	Resolution Imposed	Additional Information
					agreement policies and procedures	
Feinstein Institute for Medical Research	Covered Entity	Office for Civil Rights	• Feinstein impermissibly disclosed the ePHI of 13,000 individuals when a Feinstein-owned laptop computer containing ePHI was left unsecured in the back seat of an employee's care • Feinstein failed to conduct an accurate and through risk analysis of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all the ePHI on the laptop • Feinstein failed to implement policies and procedures for granting access to ePHI by its workforce members • Feinstein failed to implement physical	March 17th, 2016	• $3.9 million in civil monetary penalties • Corrective Active plan for 3 years requires Feinstein to conduct a risk assessment and submit the results of such risk assessment to HHS for review and approval and conduct any additional follow-up required; Implement a process to evaluate any environmental or operational changes that affect the security of ePHI; revise policies and procedures in accordance with HHS recommendations;	• Feinstein is a wholly-controlled subsidiary of Northwell Health Inc., formally known as North Shore Long Island Jewish Health System, a large health system headquartered in Manhasset, New York that is comprised of twenty one hospitals and over 450 patient facilities and physician practices

This chart summarizes certain information related to select public government settlements. It is based solely on public sources and is not an exhaustive list of HIPAA privacy and security enforcement actions.

SELECT HIPAA PRIVACY AND SECURITY ENFORCEMENT ACTIONS

Settling Party	Business Associate or Covered Entity	Enforcing Party	Alleged HIPAA Violation(s)	Date of Resolution	Resolution Imposed	Additional Information
			safeguards for the laptop to restrict access to unauthorized users • Feinstein failed to implement policies and procedures that govern receipt and removal of hardware and electronic media that contained ePHI into and out of the facility, and movement within the facility • Feinstein failed to implement mechanism to encrypt ePHI, or alternatively, document why encryption was not reasonable and appropriate		distribute revised policies and procedures to workforce; train all workforce	
North Memorial Health Care of Minnesota	Covered Entity	Office for Civil Rights	• Unencrypted, password-protected laptop was stolen from business associate workforce member's locked vehicle impacting 9,497 individuals	March 16, 2016	• $1,550,000 in civil monetary penalties • Corrective action plan (2 years) requires North Memorial to develop	• North Memorial filed a breach report on September 27, 2011

This chart summarizes certain information related to select public government settlements. It is based solely on public sources and is not an exhaustive list of HIPAA privacy and security enforcement actions.

SELECT HIPAA PRIVACY AND SECURITY ENFORCEMENT ACTIONS

Settling Party	Business Associate or Covered Entity	Enforcing Party	Alleged HIPAA Violation(s)	Date of Resolution	Resolution Imposed	Additional Information
			• OCR's investigation revealed North Memorial failed to have in place a business associate agreement • North Memorial also failed to complete a risk analysis to address all potential risks and vulnerabilities to the ePHI it maintained, accessed, or transmitted		an organization-wide risk analysis and risk management plan; also train appropriate workforce members on all policies and procedures newly developed or revised pursuant to this corrective action plan	
Lincare, Inc.	Covered Entity	U.S. Department of Health and Human Services Administrative Law Judge	• A Lincare employee removed documents containing PHI of 278 patients from a Lincare office, left the information exposed, and abandoned it • OCR's investigation revealed that Lincare had inadequate policies and procedures to safeguard PHI taken offsite • Lincare also had an unwritten policy requiring	February 2016	• $239,800 in civil monetary penalties	• This is the second time that OCR sought civil monetary penalties for HIPAA violations (both attempts were successful) • OCR's investigation began after an individual complained • Lincare claimed it had not violated HIPAA and instead PHI was

This chart summarizes certain information related to select public government settlements. It is based solely on public sources and is not an exhaustive list of HIPAA privacy and security enforcement actions.

SELECT HIPAA PRIVACY AND SECURITY ENFORCEMENT ACTIONS

Settling Party	Business Associate or Covered Entity	Enforcing Party	Alleged HIPAA Violation(s)	Date of Resolution	Resolution Imposed	Additional Information
			certain employees to store PHI in their vehicles for extended periods of time • Lincare took only minimal action to correct its policies and strengthen safeguards			stolen by the individual who discovered it; the ALJ rejected this argument
University of Washington Medicine	Covered Entity	Office for Civil Rights	• A UWM employee downloaded an email attachment containing malicious malware, which compromised the organization's IT system and the ePHI of approximately 90,000 individuals • OCR's investigation revealed that UWM did not ensure its affiliated entities were properly conducting risk assessments and responding to potential risks and vulnerabilities	December 2015	• $750,000 • Corrective Action Plan (2 years) requires: developing a current, thorough risk analysis of certain risks and vulnerabilities to the UWM facilities and submitting such analysis to HHS for approval; providing HHS with a risk management plan for approval; providing documentation regarding development and implementation of	• UWM is an affiliated Covered Entity and includes other entities under the control of the University of Washington, including University of Washington Medical Center • OCR received a breach report from UWM 11/27/13

This chart summarizes certain information related to select public government settlements. It is based solely on public sources and is not an exhaustive list of HIPAA privacy and security enforcement actions.

SELECT HIPAA PRIVACY AND SECURITY ENFORCEMENT ACTIONS

Settling Party	Business Associate or Covered Entity	Enforcing Party	Alleged HIPAA Violation(s)	Date of Resolution	Resolution Imposed	Additional Information
					reorganization of UWM compliance program to include Security Rule compliance	
University of Rochester Medical Center	Covered Entity	New York Attorney General	• In March 2015, a nurse practitioner was preparing to leave URMC for Greater Rochester Neurology. She first obtained a spreadsheet with contact information and diagnoses of 3,403 URMC patients and provided that spreadsheet to GRN. In April 2015, GRN mailed letters to those patients advising them of the nurse's departure and the option to be treated at GRN	November 2015	• $15,000 • URMC also agreed to: provide the AG with recommendations decided upon by its related task force; provide the AG with privacy, security, and breach notification policies and procedures; train its workforce; and notify the AG of any known breaches for 3 years; reporting of "reportable events" - instances of suspected noncompliance; and submission of annual	• URMC terminated the nurse and sent a breach notification letter to the patients. URM also notified HHS and the media, and received an attestation from GRN that all health information was returned or deleted. • After the breach, URMC convened a task force regarding PHI and managing departing and incoming employees.

This chart summarizes certain information related to select public government settlements. It is based solely on public sources and is not an exhaustive list of HIPAA privacy and security enforcement actions.

SELECT HIPAA PRIVACY AND SECURITY ENFORCEMENT ACTIONS

Settling Party	Business Associate or Covered Entity	Enforcing Party	Alleged HIPAA Violation(s)	Date of Resolution	Resolution Imposed	Additional Information
					reports regarding HIPAA compliance to HHS	
Triple-S Management Corporation	Covered Entity	Office for Civil Rights	• In September 2010, 2 former TSS employees retained database access rights and accessed restricted areas of a proprietary internet IPA database • In September 2013, TSS discovered that its vendor disclosed beneficiaries' PHI on a pamphlet mailed out. The vendor received such information for the pamphlets without a BAA • In April 2014, TSA discovered that its vendor disclosed beneficiaries' PHI on a pamphlet mailed out. The vendor received such information for the pamphlets without a BAA	November 2015	• $3,500,000 • Corrective Action Plan (3 years) requires: conducting a risk analysis and implementing a risk management plan; review, revision, and distribution of policies and procedures; conducting training; reporting of "reportable events" - instances of suspected noncompliance; and submission of annual reports regarding HIPAA compliance to HHS	• TSM settled on behalf of its wholly owned subsidiaries Triple-S Salud Inc., Triple-C Inc., and Triple-S Advantage Inc. • TSM is an insurance holding company based in Puerto Rico

This chart summarizes certain information related to select public government settlements. It is based solely on public sources and is not an exhaustive list of HIPAA privacy and security enforcement actions.

SELECT HIPAA PRIVACY AND SECURITY ENFORCEMENT ACTIONS

Settling Party	Business Associate or Covered Entity	Enforcing Party	Alleged HIPAA Violation(s)	Date of Resolution	Resolution Imposed	Additional Information
			• In January 2014, a former employee of a business associate downloaded beneficiary PHI and uploaded it onto his new employer's computer • In October 2014, enrollment staff mailed member ID cards to incorrect individuals • In December 2014, beneficiaries' PHI was impermissibly placed on labels used in a mailing • In January 2015, a mailing was sent to beneficiaries that included PHI for another member on the back of the letter • OCR's investigation following receipt of the above listed breach reports revealed that some or all of the companies: failed to			

This chart summarizes certain information related to select public government settlements. It is based solely on public sources and is not an exhaustive list of HIPAA privacy and security enforcement actions.

SELECT HIPAA PRIVACY AND SECURITY ENFORCEMENT ACTIONS

Settling Party	Business Associate or Covered Entity	Enforcing Party	Alleged HIPAA Violation(s)	Date of Resolution	Resolution Imposed	Additional Information
			implement appropriate safeguards; impermissibly disclosed PHI; did not comply with minimum necessary requires; failed to conduct an accurate and thorough risk analysis; and failed to implement procedures to terminate access to ePHI when an employee leaves the workforce			
Lahey Hospital and Medical Center	Covered Entity	Office for Civil Rights	• In August 2011, a laptop was stolen from an unlocked treatment room containing unencrypted PHI of 599 individuals • OCR's investigation revealed that Lahey failed to: conduct a thorough risk analysis; safeguard the workstation at issue that accessed PHI; maintain certain required policies and procedures; require	November 2015	• $850,000 • Corrective Action Plan (2 years) requires: conducting a risk analysis; developing and revising certain policies and procedures; providing training; reporting of "reportable events" - instances of	• Lahey is a nonprofit teaching hospital affiliated with Tufts Medical Center, providing primary and specialty care in MA • The stolen laptop operated a portable CT scanner and produced images for viewing through the Radiology Information System

This chart summarizes certain information related to select public government settlements. It is based solely on public sources and is not an exhaustive list of HIPAA privacy and security enforcement actions.

SELECT HIPAA PRIVACY AND SECURITY ENFORCEMENT ACTIONS

Settling Party	Business Associate or Covered Entity	Enforcing Party	Alleged HIPAA Violation(s)	Date of Resolution	Resolution Imposed	Additional Information
			use of certain usernames to access ePHI; and record activity at the workstation at issue		suspected noncompliance; and submission of annual reports regarding HIPAA compliance to HHS	• Lahey notified OCR of the stolen laptop in October 2011 • OCR informed Lahey of its investigation in November 2011
Hartford Hospital, EMC Corporation	Both	Connecticut Attorney General	• In June 2012, a laptop was stolen from an EMC employee's home containing unencrypted PHI of approximately 8,883 Connecticut residents	November 2015	• $90,000 • Both parties will augment training • Hartford Hospital is implementing corrective action regarding its vendor agreements and controls • Hartford Hospital agreed to encrypt files containing PHI prior to its transmission, when applicable • EMC agreed to maintain policies regarding encryption	• EMC was retained by Hartford Hospital to assist on a quality improvement project regarding hospital readmissions • Hartford Hospital maintained there was no evidence that the stolen information was misused • EMC notified both local enforcement and Hartford Hospital of the laptop theft • The parties never entered into a BAA • Hartford Hospital

This chart summarizes certain information related to select public government settlements. It is based solely on public sources and is not an exhaustive list of HIPAA privacy and security enforcement actions.

SELECT HIPAA PRIVACY AND SECURITY ENFORCEMENT ACTIONS

Settling Party	Business Associate or Covered Entity	Enforcing Party	Alleged HIPAA Violation(s)	Date of Resolution	Resolution Imposed	Additional Information
					of PHI and storage of PHI	notified the AG of the theft 7/13/12 and affected patients 7/30/12, as well as a media statement
Cancer Care Group, P.C.	Covered Entity	Office for Civil Rights	• In July 2012, a laptop and computer server backup media were stolen from an employee's car • Unencrypted server backup media contained the ePHI of approximately 55,000 individuals • OCR's investigation revealed that CCG failed to conduct a risk assessment prior to the breach and also failed to implement HIPAA compliant policies and procedures regarding the receipt and removal of hardware and electronic media that contain ePHI	August 2015	• $750,000 • Corrective Action Plan (3 years) requires: conducting a risk analysis and submitting such analysis to HHS; review and update of risk analysis at least annually; development and implementation of risk management plan; review and revision of HIPAA security policies and procedures; review and revision of HIPAA security training; reporting of	• CCG submitted a breach report 8/29/12 • Stolen ePHI included names, addresses, dates of birth, Social Security numbers, insurance information, and clinical information

This chart summarizes certain information related to select public government settlements. It is based solely on public sources and is not an exhaustive list of HIPAA privacy and security enforcement actions.

SELECT HIPAA PRIVACY AND SECURITY ENFORCEMENT ACTIONS

Settling Party	Business Associate or Covered Entity	Enforcing Party	Alleged HIPAA Violation(s)	Date of Resolution	Resolution Imposed	Additional Information
					"reportable events" - instances of suspected noncompliance; submission of annual reports regarding HIPAA compliance to HHS	
St. Elizabeth's Medical Center	Covered Entity	Office for Civil Rights	• SEMC used an internet based document sharing application to store PHI of at least 498 individuals without first analyzing risks • SEMC suffered a breach of 595 individuals' PHI that was improperly stored on a former workforce member's personal laptop and flash drive • OCR's investigation revealed that SEMC did not properly respond to a known security incident	July 2015	• $218,400 • Corrective Action Plan (1 year) requires: conducting a compliance self-assessment; updating HIPAA policies, procedures, and training as needed; and reporting of "reportable events" - instances of suspected noncompliance	• OCR received a complaint regarding internet document sharing 11/16/12 and investigated • OCR separately received a breach report regarding former workforce member's laptop and flash drive 8/25/14 and investigated
Cornell	Covered	Office for Civil	• Cornell disposed of	April 2015	• $125,000	• Cornell is a small

This chart summarizes certain information related to select public government settlements. It is based solely on public sources and is not an exhaustive list of HIPAA privacy and security enforcement actions.

SELECT HIPAA PRIVACY AND SECURITY ENFORCEMENT ACTIONS

Settling Party	Business Associate or Covered Entity	Enforcing Party	Alleged HIPAA Violation(s)	Date of Resolution	Resolution Imposed	Additional Information
Prescription Pharmacy	Entity	Rights	unsecured documents containing PHI of 1,610 patients in unlocked, open dumpster accessible to the public • OCR's investigation revealed that Cornell had not implemented written policies and procedures required by the HIPAA Privacy Rule, nor had Cornell provided training to its workforce		• Corrective Action Plan (2 years) requires: developing written HIPAA policies and procedures and providing such documents to HHS for approval; training of the workforce; and reporting of "reportable events" - instances of suspected noncompliance	pharmacy that provides in-store and prescription services to patients in Denver, CO; they specialize in compounded medications and services for hospice care agencies • OCR opened investigation 1/13/12 after receiving notification from a local Denver news outlet regarding the disposal of unsecured documents containing PHI • OCR notified Cornell of its investigation 2/27/12
Anchorage Community Mental Health Services	Covered Entity	Office for Civil Rights	• Malware compromised the security of IT resources, affecting the unsecured ePHI of 2,743 individuals	December 2014	• $150,000 • Corrective Action Plan (2 years)	• ACMHS submitted security breach report in March 2012

This chart summarizes certain information related to select public government settlements. It is based solely on public sources and is not an exhaustive list of HIPAA privacy and security enforcement actions.

SELECT HIPAA PRIVACY AND SECURITY ENFORCEMENT ACTIONS

Settling Party	Business Associate or Covered Entity	Enforcing Party	Alleged HIPAA Violation(s)	Date of Resolution	Resolution Imposed	Additional Information
			• OCR's investigation revealed that ACMHS adopted security policies in 2005 but did not follow them • AMHS failed to regularly update IT resources with security patches and ran outdated software		requires: revising and distributing security policies and procedures; performing training; annually conducting a risk analysis; and reporting of "reportable events" - instances of suspected noncompliance	• OCR notified ACMHS of its investigation in June 2012
Beth Israel Deaconess Medical Center	Covered Entity	Massachusetts Attorney General	• In May 2012, physically unsecured laptop containing personal information of nearly 4,000 patients and employees was stolen • Laptop was not safeguarded; employees did not follow hospital policy to encrypt and physically secure laptop	November 2014	• $100,000 ($70,000 civil penalty; $14,000 for attorney's fees and costs; $15,000 payment to an educational fund concerning protection of personal information)	• Information stolen included names, Social Security numbers, and health information • Although Breach occurred in May 2012, patients were not notified until August 2012 • Beth Israel has already enhanced its data security practices; they now encrypt all

This chart summarizes certain information related to select public government settlements. It is based solely on public sources and is not an exhaustive list of HIPAA privacy and security enforcement actions.

SELECT HIPAA PRIVACY AND SECURITY ENFORCEMENT ACTIONS

Settling Party	Business Associate or Covered Entity	Enforcing Party	Alleged HIPAA Violation(s)	Date of Resolution	Resolution Imposed	Additional Information
						devices prior to usage
Women & Infants Hospital of Rhode Island	Covered Entity	Massachusetts Attorney General	• In 2011, W&I lost 19 unencrypted backup tapes sent to its prenatal diagnostics centers located in both Rhode Island and Massachusetts	July 2014	• $150,000 ($110,000 civil penalty; $25,000 for fees and costs; $15,000 for future data security litigation fund and fund to promote education on protecting personal information) • Mandatory improvement of data security compliance program	• W&I reported issue to Massachusetts AG in fall 2012 when they realized the tapes were missing • Tapes contained Social Security numbers, physicians' names, ultrasound images, and other information of 12,127 Massachusetts residents
Parkview Health System, Inc.	Covered Entity	Office for Civil Rights	• In June 2009, Parkview employees left 71 boxes of medical records unattended on a physician's home driveway within 20 feet of a public road despite having notice that the physician was not home	June 2014	• $800,000 • Corrective Action Plan (1 year) requires: developing written policies and procedures regarding administrative, physical, and technical safeguards	• Physician issued complaint with OCR on June 10, 2009 • OCR opened investigation of Parkview on May 16, 2011 • Parkview had taken custody of medical

This chart summarizes certain information related to select public government settlements. It is based solely on public sources and is not an exhaustive list of HIPAA privacy and security enforcement actions.

SELECT HIPAA PRIVACY AND SECURITY ENFORCEMENT ACTIONS

Settling Party	Business Associate or Covered Entity	Enforcing Party	Alleged HIPAA Violation(s)	Date of Resolution	Resolution Imposed	Additional Information
					to protect the privacy of non-electronic PHI; developing a comprehensive training program; investigation and reporting of "reportable events" - instances of suspected noncompliance	records of between 5,000 and 8,000 of physician's patients as they helped to transition patients to new providers
Columbia University	Covered Entity	Office for Civil Rights	• Computer server was errantly reconfigured, which resulted in the disclosure of the ePHI of 6,800 patients to internet search engines • OCR's investigation also found lack of comprehensive risk analysis and failure to implement processes to asses and monitor IT equipment, applications, and data systems	May 2014	• $1,500,000 • Corrective Action Plan (3 years) requires: conducting a risk analysis; developing a risk management plan; revising policies and procedures; developing a process to evaluate environmental or operational changes affecting ePHI	• NYP/CU discovered matter when partner of deceased patient found patient's PHI online and complained • NYP/CU filed breach report 9/27/10 • 11/5/10 OCR notified of investigation

This chart summarizes certain information related to select public government settlements. It is based solely on public sources and is not an exhaustive list of HIPAA privacy and security enforcement actions.

SELECT HIPAA PRIVACY AND SECURITY ENFORCEMENT ACTIONS

Settling Party	Business Associate or Covered Entity	Enforcing Party	Alleged HIPAA Violation(s)	Date of Resolution	Resolution Imposed	Additional Information
					security; developing training program; investigation and reporting of "reportable events" - instances of suspected noncompliance	
New York and Presbyterian	Covered Entity	Office for Civil Rights	• Computer server was errantly reconfigured, which resulted in the disclosure of the ePHI of 6,800 patients to internet search engines • OCR's investigation also found lack of comprehensive risk analysis; insufficient processes to access and monitor IT equipment and data systems; insufficient security measures; failure to implement and follow appropriate policies and procedures for authorizing	May 2014	• $3,300,000 • Corrective Action Plan (3 years) requires: conducting a risk analysis; developing a risk management plan; revising policies and procedures; developing a process to evaluate environmental or operational changes affecting ePHI security; augmenting training program; investigation and	• NYP/CU discovered matter when partner of deceased patient found patient's PHI online and complained • NYP/CU filed breach report 9/27/10 • 11/5/10 OCR notified of investigation

This chart summarizes certain information related to select public government settlements. It is based solely on public sources and is not an exhaustive list of HIPAA privacy and security enforcement actions.

SELECT HIPAA PRIVACY AND SECURITY ENFORCEMENT ACTIONS

Settling Party	Business Associate or Covered Entity	Enforcing Party	Alleged HIPAA Violation(s)	Date of Resolution	Resolution Imposed	Additional Information
			access to patient databases		reporting of "reportable events" - instances of suspected noncompliance	
Concentra Health Services	Covered Entity	Office for Civil Rights	• Unencrypted laptop containing ePHI was stolen from a physical therapy center in Springfield, Missouri • Concentra had previously identified that lack of encryption was a "critical risk," but efforts to encrypt were incomplete and inconsistent • OCR's investigation also found that Concentra had insufficient security management processes in place	April 2014	• $1,725,220 • Corrective Action Plan (2 years) requires: completing a risk analysis and risk management plan; evidence of all implemented and planned remediation actions; providing update to OCR regarding encryption status, including an explanation for devices and equipment that are not encrypted	• Concentra submitted security breach report in December 2011 • OCR opened its investigation in in May 2012
QCA Health Plan, Inc.	Covered Entity	Office for Civil Rights	• Unencrypted laptop containing ePHI of 148	April 2014	• $250,000 • Corrective Action	• QCA submitted security breach report

This chart summarizes certain information related to select public government settlements. It is based solely on public sources and is not an exhaustive list of HIPAA privacy and security enforcement actions.

SELECT HIPAA PRIVACY AND SECURITY ENFORCEMENT ACTIONS

Settling Party	Business Associate or Covered Entity	Enforcing Party	Alleged HIPAA Violation(s)	Date of Resolution	Resolution Imposed	Additional Information
			individuals was stolen from an employee's car • OCR's investigation also found that QCA failed to comply with multiple requirements of HIPAA		Plan (2 years) requires: completing a risk analysis and risk management plan; workforce training; investigation and reporting of "reportable events" - instances of suspected noncompliance	in February 2012 • OCR notified QCA of investigation in May 2012
Skagit County, WA	Covered Entity	Office for Civil Rights	• ePHI of 1,581 individuals, some of which related to testing and treatment for infectious diseases, was inadvertently moved to one of Skagit County's public-access servers • Information was searchable on Google and publicly available online for 14 days in September 2011 • OCR's investigation revealed additional noncompliance with HIPAA,	March 2014	• $215,000 • Corrective Action Plan (3 years) requires: substitute Breach notification to affected individuals previously not notified; updated accountings of disclosures of PHI for affected individuals; documentation of hybrid entity status; approval of BAAs; risk	• OCR opened its investigation after receiving a Breach report in 2011 that money receipts with seven individuals' ePHI had been accessed by unknown parties • First settlement between OCR and a county government • Skagit County's Public Health Department

This chart summarizes certain information related to select public government settlements. It is based solely on public sources and is not an exhaustive list of HIPAA privacy and security enforcement actions.

SELECT HIPAA PRIVACY AND SECURITY ENFORCEMENT ACTIONS

Settling Party	Business Associate or Covered Entity	Enforcing Party	Alleged HIPAA Violation(s)	Date of Resolution	Resolution Imposed	Additional Information
			including failure to: provide breach notification to affected individuals; implement policies and procedures for HIPAA compliance; and provide training to workforce members		analysis and risk management plan; revised policies and procedures; workforce training; investigation and reporting of "reportable events" - instances of suspected noncompliance	provides essential services to those who otherwise would not be able to afford health care
Adult & Pediatric Dermatology PC (APDerm)	Covered Entity	Office for Civil Rights	• Following October 2011 theft of flash drive containing ePHI of ~2,200 individuals, although APDerm timely notified patients, they did not conduct an accurate and thorough analysis of potential risks and vulnerabilities until October 2012 • Did not have written policies and procedures in place	December 2013	• $150,000 • Corrective Action Plan requires: risk analysis and risk management plan; revised policies and procedures; submission to OCR of Implementation Report – the acceptance of which signifies the end of the CAP	• OCR opened investigation after receiving report from APDerm in October 2011 that unencrypted flash drive containing ePHI of approximately 2,200 individuals was stolen from an employee's car • APDerm said flash drive did not contain sensitive health

This chart summarizes certain information related to select public government settlements. It is based solely on public sources and is not an exhaustive list of HIPAA privacy and security enforcement actions.

SELECT HIPAA PRIVACY AND SECURITY ENFORCEMENT ACTIONS

Settling Party	Business Associate or Covered Entity	Enforcing Party	Alleged HIPAA Violation(s)	Date of Resolution	Resolution Imposed	Additional Information
			• Did not train workforce members			information or financial information • Flash drive was never used to anyone's knowledge
AvMed, Inc.	Covered Entity	Class Action Lawsuit	• Maintained insufficient data security safeguards that led to the 2009 theft of laptops containing PHI of 1.2 million customers	October 2013; received final approval February 2014	• $3,000,000 • AvMed also agreed to: implement security training for all employees, train employees on appropriate laptop use, increase security regarding company laptops, adopt full disk encryption technology on all company computers, and upgrade physical security at company facilities	• Dispute dates back to December 2010 when initial lawsuit was filed following theft of two unencrypted laptops • Lawsuit was dismissed in July 2011 due to plaintiffs failing to show cognizable injury • Lawsuit was revived in September 2012 by the Eleventh Circuit which said the lawsuit should proceed since the plaintiffs linked stolen materials to subsequent opening of bogus bank accounts

This chart summarizes certain information related to select public government settlements. It is based solely on public sources and is not an exhaustive list of HIPAA privacy and security enforcement actions.

SELECT HIPAA PRIVACY AND SECURITY ENFORCEMENT ACTIONS

Settling Party	Business Associate or Covered Entity	Enforcing Party	Alleged HIPAA Violation(s)	Date of Resolution	Resolution Imposed	Additional Information
						• Members of the class may make claims from the settlement fund to recover losses
Affinity Health Plan, Inc.	Covered Entity	Office for Civil Rights	• Impermissibly disclosed the PHI of up to 344,579 individuals by returning multiple photocopiers to a leasing agent prior to erasing data contained on their hard drives • Did not identify potential security risks of ePHI stored on copiers' hard drives • Did not implement ePHI disposal policies when returning copiers	August 2013	• $1,215,780 • Corrective Action Plan (120 days) requires Affinity Health Plan ("AHP") to, within 5 days of Effective Date, use best efforts to retrieve all copier hard drives that remain in possession of Canon Financial Services and safeguard all ePHI contained therein. AHP shall provide OCR with written certification of success or explain best efforts and reason that it cannot	• AHP is a not-for-profit managed care plan serving the New York metropolitan area • OCR received Breach notification from AHP on April 15, 2010; OCR notified AHP of pending investigation on May 19, 2010 • AHP was informed by a representative from CBS that, as part of an investigatory report, CBS had purchased a copier previously leased by Affinity, and the copier contained confidential medical information

This chart summarizes certain information related to select public government settlements. It is based solely on public sources and is not an exhaustive list of HIPAA privacy and security enforcement actions.

SELECT HIPAA PRIVACY AND SECURITY ENFORCEMENT ACTIONS

Settling Party	Business Associate or Covered Entity	Enforcing Party	Alleged HIPAA Violation(s)	Date of Resolution	Resolution Imposed	Additional Information
					retrieve hard drives. AHP shall also, within 30 days of Effective Date, conduct a comprehensive risk analysis and mitigate risks identified. AHP may request an extension of time.	
WellPoint, Inc.	Covered Entity	Office for Civil Rights	• Security weaknesses in an online application database left ePHI (including names, dates of birth, addresses, Social Security numbers, phone numbers, and health information) of ~612,000 individuals accessible to unauthorized individuals over the internet • Did not adequately implement policies and procedures regarding access to online application database • Did not appropriately	July 2013	• $1,700,000	• Investigation began following WellPoint's June 2010 submission of a HIPAA Breach report • WellPoint entered Resolution Agreement on behalf of the health plans under its common ownership or control that have been designated as a single Affiliated Covered Entity • No Corrective Action Plan included in

This chart summarizes certain information related to select public government settlements. It is based solely on public sources and is not an exhaustive list of HIPAA privacy and security enforcement actions.

SELECT HIPAA PRIVACY AND SECURITY ENFORCEMENT ACTIONS

Settling Party	Business Associate or Covered Entity	Enforcing Party	Alleged HIPAA Violation(s)	Date of Resolution	Resolution Imposed	Additional Information
			evaluate potential technical risks following software upgrade • Did not have safeguards in place to verify identify of those seeking access to ePHI in online application database			Resolution Agreement
Shasta Regional Medical Center and other Prime Healthcare Services facilities	Covered Entity	Office for Civil Rights	• Impermissible release of a patient's medical records to the media • Impermissible disclosure of patient's PHI to entire workforce and medical staff (785 – 900 individuals) without written authorization • Failure to sanction workforce members for HIPAA violations	June 2013	• $275,000 • Corrective Action Plan (1 year) requires: revision of policies and procedures; reporting of "reportable events" – when a workforce member may have failed to comply with HIPAA policies and procedures; training; submission of Implementation Report and Annual Report regarding	• Shasta Regional Medical Center ("SRMC") was aiming to respond to a California Watch story regarding allegations that SRMC was overbilling Medicare • DOJ investigation into Prime's billing practices is ongoing • OCR investigation followed *Los Angeles Times* January 4, 2012 article discussing impermissible

This chart summarizes certain information related to select public government settlements. It is based solely on public sources and is not an exhaustive list of HIPAA privacy and security enforcement actions.

SELECT HIPAA PRIVACY AND SECURITY ENFORCEMENT ACTIONS

Settling Party	Business Associate or Covered Entity	Enforcing Party	Alleged HIPAA Violation(s)	Date of Resolution	Resolution Imposed	Additional Information
					compliance with Corrective Action Plan	disclosure of PHI • California Department of Public Health also fined Prime in November 2012 (see below)
Idaho State University (operates outpatient clinics)	Covered Entity	Office for Civil Rights	• Firewall protections at servers maintained by Idaho State University ("ISU") were disabled for maintenance purposes and not restored properly, leaving the ePHI of ~17,500 patients unsecured for at least 10 months • Numerous additional potential HIPAA violations occurred between 2007 and 2012, including failure to conduct a risk analysis of ePHI; inadequate implementation of security measures; and inadequate review of information systems activity	May 2013	• $400,000 • Corrective Action Plan (2 years) requires: risk management plan including specific security measures; documentation of implementation of policies and procedures regarding information systems activity review; documentation of an updated compliance gap analysis that includes a contingency plan and a listing of technical	• Investigation began following Breach report in August 2011

This chart summarizes certain information related to select public government settlements. It is based solely on public sources and is not an exhaustive list of HIPAA privacy and security enforcement actions.

SELECT HIPAA PRIVACY AND SECURITY ENFORCEMENT ACTIONS

Settling Party	Business Associate or Covered Entity	Enforcing Party	Alleged HIPAA Violation(s)	Date of Resolution	Resolution Imposed	Additional Information
					safeguards	
Goldthwait Associates and 4 pathology groups	Covered Entities	Massachusetts Attorney General	• Disposed of medical records and confidential billing information of over 67,000 Massachusetts patients at a public dump	January 2013	• $140,000 (collectively)	• Goldthwait Associates is a medical billing practice • Other defendants are: Dr. Kevin Dole, former president of Chestnut Pathology Services, P.C.; Milford Pathology Associates, P.C.; Milton Pathology Associates, P.C.; and Pioneer Valley Pathology Associates, P.C. • In July 2010, a Boston Globe photographer found medical records in the public dump • HIPAA and state data security law implicated • Pathology practices implicated for failing to take reasonable steps to select and retain a

This chart summarizes certain information related to select public government settlements. It is based solely on public sources and is not an exhaustive list of HIPAA privacy and security enforcement actions.

SELECT HIPAA PRIVACY AND SECURITY ENFORCEMENT ACTIONS

Settling Party	Business Associate or Covered Entity	Enforcing Party	Alleged HIPAA Violation(s)	Date of Resolution	Resolution Imposed	Additional Information
						service provider that would properly secure sensitive information
Hospice of North Idaho	Covered Entity	Office for Civil Rights	• Unencrypted laptop containing ePHI of 441 patients was stolen in June 2010 • Hospice of North Idaho ("HONI") did not conduct a risk analysis to safeguard ePHI and did not have in place policies and procedures regarding mobile device security	January 2013	• $50,000 • Corrective Action Plan (2 years) requires reporting of "reportable events" – when a workforce member may have failed to comply with HIPAA policies and procedures	• Investigation began following Breach report • HONI took steps to improve HIPAA compliance following June theft • First OCR settlement involving a Breach of unsecured ePHI affecting fewer than 500 individuals
Prime Healthcare Services	Covered Entity	California Department of Public Health	• Improper disclosure of a patient's medical files to the media and all employees of Shasta Regional Medical Center ("SRMC")	November 2012	• $95,000	• California Department of Public Health said that it issued an additional $3,100 in penalties due to SRMC's failure to report the disclosure in a timely manner • Prime Healthcare Services ("Prime") has

This chart summarizes certain information related to select public government settlements. It is based solely on public sources and is not an exhaustive list of HIPAA privacy and security enforcement actions.

SELECT HIPAA PRIVACY AND SECURITY ENFORCEMENT ACTIONS

Settling Party	Business Associate or Covered Entity	Enforcing Party	Alleged HIPAA Violation(s)	Date of Resolution	Resolution Imposed	Additional Information
						appealed the state findings and penalties • OCR also penalized Prime for alleged HIPAA violations in June 2013 (see above) • Patient sued Prime for wrongful disclosure of PHI in January 2013
Massachusetts Eye and Ear Infirmary and Massachusetts Eye and Ear Associates Inc.	Covered Entity	Office for Civil Rights	• Theft of unencrypted personal laptop containing ePHI of Massachusetts Eye and Ear ("MEEI") patients and research subjects • Did not analyze risk to ePHI maintained on portable devices, implement security measures to protect ePHI, or implement appropriate policies and procedures	September 2012	• $1,500,000 • Corrective Action Plan (3 years) requires: review, revision, and distribution of policies and procedures; investigation and report following receipt of information that a workforce member may have failed to comply with HIPAA;	• Investigation began following Breach report

This chart summarizes certain information related to select public government settlements. It is based solely on public sources and is not an exhaustive list of HIPAA privacy and security enforcement actions.

SELECT HIPAA PRIVACY AND SECURITY ENFORCEMENT ACTIONS

Settling Party	Business Associate or Covered Entity	Enforcing Party	Alleged HIPAA Violation(s)	Date of Resolution	Resolution Imposed	Additional Information
					training; designation of an independent monitor and monitor reporting	
Alaska Department of Health and Social Services	Covered Entity	Office for Civil Rights	• USB with PHI of Medicaid beneficiaries stolen from employee's car • Did not conduct risk analyses, implement risk management measures, complete security training, implement device and media controls, or address device and media encryption • Did not have adequate policies and procedures in place to safeguard ePHI	June 2012	• $1,700,000 • Corrective Action Plan (3 years) requires: review, revision, adoption, and distribution of policies and procedures; training; risk analysis and adoption of risk management measures; designation of an independent monitor and monitor reporting	• Alaska Department of Health and Social Services ("DHSS") reported Breach in October 2009 • First OCR enforcement vs. a state
South Shore Hospital	Covered Entity	Massachusetts Attorney General (settlement for both HIPAA	• Hospital shipped boxes containing 473 unencrypted backup computer tapes with PHI of	May 2012	• $250,000 civil penalty • $225,000 contribution to Attorney General's	• South Shore Hospital reported issue to Massachusetts Attorney General in July 2010

This chart summarizes certain information related to select public government settlements. It is based solely on public sources and is not an exhaustive list of HIPAA privacy and security enforcement actions.

SELECT HIPAA PRIVACY AND SECURITY ENFORCEMENT ACTIONS

Settling Party	Business Associate or Covered Entity	Enforcing Party	Alleged HIPAA Violation(s)	Date of Resolution	Resolution Imposed	Additional Information
		and MA state law)	800,000 individuals to Archive Data Solutions to erase the tapes and resell them. Hospital did not inform vendor that PHI was on the tapes, nor did they analyze vendor's safeguards in place or enter into a BAA. Only 1 box arrived at vendor. • Failed to implement appropriate safeguards, policies, and procedures		Education Fund to promote protection of personal information • $275,000 credit to reflect security measures taken following the Breach • Corrective Action Plan requires: Massachusetts Attorney General review of information security plan; internal annual review of security measures; annual training; and hiring a third party to audit both security and agreements with data destruction services	• No reports of unauthorized use of missing PHI
Phoenix Cardiac Surgery	Covered Entity	Office for Civil Rights	• Appointments available to public on internet calendar	April 2012	• $100,000 • Corrective Action	• Entity has < 10 physicians

This chart summarizes certain information related to select public government settlements. It is based solely on public sources and is not an exhaustive list of HIPAA privacy and security enforcement actions.

SELECT HIPAA PRIVACY AND SECURITY ENFORCEMENT ACTIONS

Settling Party	Business Associate or Covered Entity	Enforcing Party	Alleged HIPAA Violation(s)	Date of Resolution	Resolution Imposed	Additional Information
			• No HIPAA policies; no documentation of employee training; limited safeguards; no identification of security official; no security risk analysis; insufficient BAAs		Plan (1 year) requires: development, revision, and distribution of policies and procedures; training; reporting to HHS upon the determination that a member of the workforce has violated HIPAA	• OCR stated that it hoped providers understood that "OCR expects full compliance no matter the size" of the Covered Entity
Blue Cross Blue Shield of Tennessee	Covered Entity	Office for Civil Rights	• 57 unencrypted computer drives containing PHI of > 1 million people were stolen from storage locker leased by Blue Cross Blue Shield of Tennessee ("BCBST") • BCBST did not perform security evaluation following operational changes	March 2012	• $1,500,000 • Corrective Action Plan (450 days) requires: submitting policies to HHS for review and approval and distributing to all members of workforce; training; monitor reviews under the direction of the Chief Privacy	• Leased data closet was secured by biometric and keycard scan security in a building with additional security • OCR's first enforcement action against an entity that voluntarily filed a Breach report • BCBST reported that it spent ~$17 million in investigation,

This chart summarizes certain information related to select public government settlements. It is based solely on public sources and is not an exhaustive list of HIPAA privacy and security enforcement actions.

SELECT HIPAA PRIVACY AND SECURITY ENFORCEMENT ACTIONS

Settling Party	Business Associate or Covered Entity	Enforcing Party	Alleged HIPAA Violation(s)	Date of Resolution	Resolution Imposed	Additional Information
					Officer; reporting to HHS upon the determination that a member of the workforce has violated HIPAA	notification, and protection efforts
Accretive Health, Inc.	Business Associate	Minnesota Attorney General	• Laptop was stolen that contained about 23,500 patients' records	January 2012	• $2,500,000 – placed in a restitution fund for patients • Accretive barred from doing business in Minnesota for 2 years, and for the following 4 years, can only re-enter Minnesota with permission of the Attorney General and after entering into a consent decree	• Accretive is a Chicago debt collector that managed the revenue operations of several Minnesota hospitals • First HIPAA enforcement action against a Business Associate • State debt collection law also involved
University of California at Los Angeles Health System	Covered Entity	Office for Civil Rights	• Employees without a job related reason to do so viewed the charts of 2 celebrity patients	July 2011	• $865,000 • Corrective Action Plan (3 years) requires: review,	• Complaints filed with OCR on behalf of 2 celebrity patients

This chart summarizes certain information related to select public government settlements. It is based solely on public sources and is not an exhaustive list of HIPAA privacy and security enforcement actions.

SELECT HIPAA PRIVACY AND SECURITY ENFORCEMENT ACTIONS

Settling Party	Business Associate or Covered Entity	Enforcing Party	Alleged HIPAA Violation(s)	Date of Resolution	Resolution Imposed	Additional Information
			• During investigation, OCR found that from 2005 – 2008, this happened repeatedly		revision, and distribution of policies and procedures; training; designation of an independent monitor to ensure Corrective Action Plan compliance	
The General Hospital Corporation and Massachusetts General Physicians Organization, Inc.	Covered Entity	Office for Civil Rights	• General Hospital Corporation ("MGH") employee left PHI of 192 patients (at least some of whom had HIV/AIDS) on subway; never recovered information • MGH failed to implement reasonable, appropriate safeguards to protect the privacy of PHI when removed from premises	February 2011	• $1,000,000 • Corrective Action Plan (3 years) that requires: development, revision, and distribution of policies and procedures; training; designation of a monitor to ensure Corrective Action Plan compliance	• Patient filed complaint with OCR
Cignet Health of Prince George's	Covered Entity	U.S. Department of Health and	• Denied 41 patients access to their medical records	Cignet notified of Civil Monetary	• $4,351,600	• First CMP issued by OCR for violations of

This chart summarizes certain information related to select public government settlements. It is based solely on public sources and is not an exhaustive list of HIPAA privacy and security enforcement actions.

SELECT HIPAA PRIVACY AND SECURITY ENFORCEMENT ACTIONS

Settling Party	Business Associate or Covered Entity	Enforcing Party	Alleged HIPAA Violation(s)	Date of Resolution	Resolution Imposed	Additional Information
County, MD		Human Services Administrative Law Judge	between September 2008 and October 2009 • Refused to respond to OCR's demands to produce the records • Failed to cooperate with OCR's investigations, including failure to respond to subpoena	Penalty in October 2010; Notice of Final Determination issued February 2011		the Privacy Rule • Patients filed complaints with HHS • OCR filed a petition to enforce its subpoena and obtained default judgment against Cignet on March 30, 2010; Cignet produced the records on April 7, 2010
Health Net, Inc. and Health Net of the Northeast, Inc.	Covered Entity	Vermont Attorney General	• Hard drive containing unencrypted PHI of 1.5 million members, including 525 Vermonters, disappeared • Health Net did not begin notifying affected Vermont residents until more than 6 months later	January 2011	• $55,000 • Health Net must: submit to data security audit; file reports with state regarding security programs for 2 years	• Parent company Health Net in Los Angeles issued a November 2009 report regarding the May 2009 hard drive disappearance to insurance officials in 4 states • Health Net claimed that files were not easily accessible, although they were in TIF format, which can be viewed

This chart summarizes certain information related to select public government settlements. It is based solely on public sources and is not an exhaustive list of HIPAA privacy and security enforcement actions.

SELECT HIPAA PRIVACY AND SECURITY ENFORCEMENT ACTIONS

Settling Party	Business Associate or Covered Entity	Enforcing Party	Alleged HIPAA Violation(s)	Date of Resolution	Resolution Imposed	Additional Information
						using certain freely available software • Vermont's first enforcement action under the Security Breach Notice Act • Connecticut Attorney General filed similar complaint in July 2010 (see below) • Complaint alleges violations of HIPAA, Vermont's Security Breach Notice Act, and Consumer Fraud Act
Management Services Organization Washington, Inc.	Covered Entity	Office for Civil Rights	• Management Services organization ("MSO") intentionally did not have in place or implement administrative, technical, or physical safeguards to protect PHI and disclosed PHI to Washington Practice Management (owned by	December 2010	• $35,000 • Corrective Action Plan (2 years) requires: development, revision, and distribution of policies and procedures; training;	

This chart summarizes certain information related to select public government settlements. It is based solely on public sources and is not an exhaustive list of HIPAA privacy and security enforcement actions.

SELECT HIPAA PRIVACY AND SECURITY ENFORCEMENT ACTIONS

Settling Party	Business Associate or Covered Entity	Enforcing Party	Alleged HIPAA Violation(s)	Date of Resolution	Resolution Imposed	Additional Information
			MSO) which used the PHI for marketing purposes		monitor reviews to be conducted by the Privacy or Security Officer	
Rite Aid Corporation (and its 40 affiliated entities)	Covered Entity	Office for Civil Rights	• Disposed of prescriptions and labeled pill bottles containing PHI in publicly accessible trash containers • Failed to implement adequate policies and procedures regarding disposal of PHI and failed to train on proper disposal	July 2010	• $1,000,000 • Corrective Action Plan (3 years) requires: development, revision, and distribution of policies and procedures; training; internal monitoring through the Compliance Representative; engagement of a third party assessor to assess Corrective Action Plan compliance	• Coordinated action with FTC to settle potential violations of FTC Act • Applies to all ~4,800 Rite Aid retail pharmacies • OCR opened investigation after TV media taped incidents showing pharmacies disposing of prescription bottles containing PHI in public industrial trash containers
Health Net of Connecticut, Inc.	Covered Entity	Connecticut Attorney General	• Parent company Health Net in Los Angeles in November	July 2010	• $250,000 fine to state	• First lawsuit by a state's chief legal officer to

This chart summarizes certain information related to select public government settlements. It is based solely on public sources and is not an exhaustive list of HIPAA privacy and security enforcement actions.

SELECT HIPAA PRIVACY AND SECURITY ENFORCEMENT ACTIONS

Settling Party	Business Associate or Covered Entity	Enforcing Party	Alleged HIPAA Violation(s)	Date of Resolution	Resolution Imposed	Additional Information
			2009 reported to insurance officials in 4 states the May 2009 disappearance of a hard drive containing unencrypted PHI of 1.5 million members, including 446,000 in Connecticut • Health Net delayed notifying consumers and law enforcement authorities		• Health Net must obtain $1,000,000 of identity theft insurance • Health Net must pay $500,000 in the event that the lost data is misused • Provision of 2 years of credit monitoring services to affected members • State approved Corrective Action Plan that requires improvement of data and equipment security	prosecute HIPAA privacy and security violations • Vermont Attorney General filed similar complaint in January 2011 (see above)
CVS Pharmacy, Inc.	Covered Entity	Office for Civil Rights	• Failed to safeguard PHI during disposal process • Failed to train employees on safe disposal of PHI	January 2009	• $2,250,000 • Corrective Action Plan (3 years) requires: development, revision, and	• Coordinated action in which parent company also signed a consent order with the FTC to settle potential violations of FTC Act

This chart summarizes certain information related to select public government settlements. It is based solely on public sources and is not an exhaustive list of HIPAA privacy and security enforcement actions.

SELECT HIPAA PRIVACY AND SECURITY ENFORCEMENT ACTIONS

Settling Party	Business Associate or Covered Entity	Enforcing Party	Alleged HIPAA Violation(s)	Date of Resolution	Resolution Imposed	Additional Information
					distribution of policies and procedures; training; internal monitoring; engagement of a third party assessor to assess Corrective Action Plan compliance	• Applies to all CVS retail pharmacies (> 6,300 stores) • OCR opened investigation after media reports alleged that PHI was being disposed in unsecured dumpsters
Providence Health & Services (Seattle)	Covered Entity	Office for Civil Rights	• Backup tapes, disks, and laptops containing PHI of > 386,000 patients were taken out of home health care operations and lost or stolen	July 2008	• $100,000 • Corrective Action Plan (3 years) that requires: revision and distribution of policies and procedures; training; monitoring under the direction of the Chief Information Security Officer	• Specific entities involved: Providence Home and Community Services; Providence Hospice and Home Care • First time HHS required a Resolution Agreement from a Covered Entity • HHS received > 30 complaints from patients after they had been alerted of the loss or theft

This chart summarizes certain information related to select public government settlements. It is based solely on public sources and is not an exhaustive list of HIPAA privacy and security enforcement actions.

SELECT HIPAA PRIVACY AND SECURITY ENFORCEMENT ACTIONS

This chart summarizes certain information related to select public government settlements. It is based solely on public sources and is not an exhaustive list of HIPAA privacy and security enforcement actions.

attorney advertisement